MADHA ENGINEERING COLLEGE

(Affiliated to Anna University and Approved by AICTE, New Delhi)
Madha Nagar, Kundrathur, Chennai-600069

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

CS8711– CLOUD COMPUTING LABORATORY

R 2017
LAB MANUAL

INDEX

EX.NO 1:

DATE :

INSTALL VIRTUALBOX/VMWARE WORKSTATION WITH DIFFERENT FLAVOURS OF LINUX OR WINDOWS OS ON TOP OF WINDOWS7 OR 8

Aim:

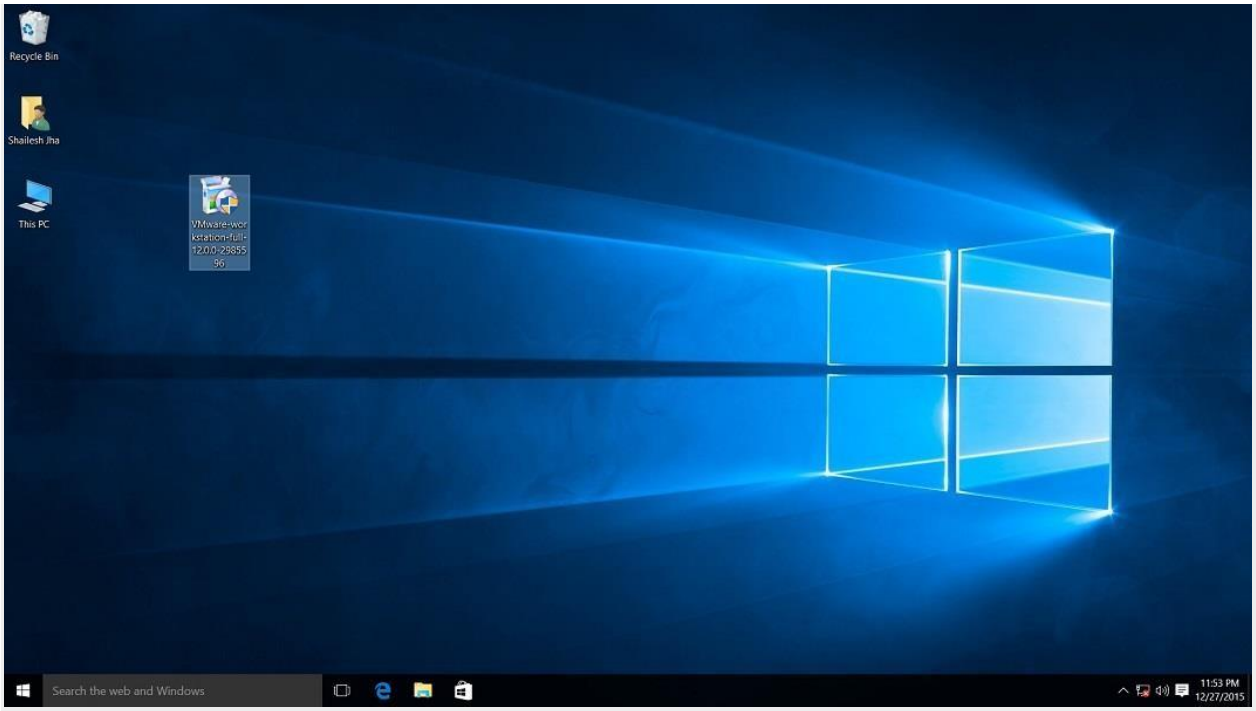
Find procedure to Install Virtualbox/VMware Workstation with different flavours of linux or windows OS on top of windows7 or 8.

PROCEDURE TO INSTALL

Step 1- Download Link
Link for downloading the software is https://www.vmware.com/products/workstation-pro/workstation-pro-evaluation.html. Download the software for windows. Good thing is that there is no signup process. Click and download begins. Software is around 541 MB.

Step 2- Download the installer file
It should probably be in the download folder by default, if you have not changed the settings in your browser. File name should be something like VMware-workstation-full-15.5.1-15018445.exe. This file name can change depending on the version of the software currently available for download. But for now, till the next version is available, they will all be VMware Workstation 15 Pro.

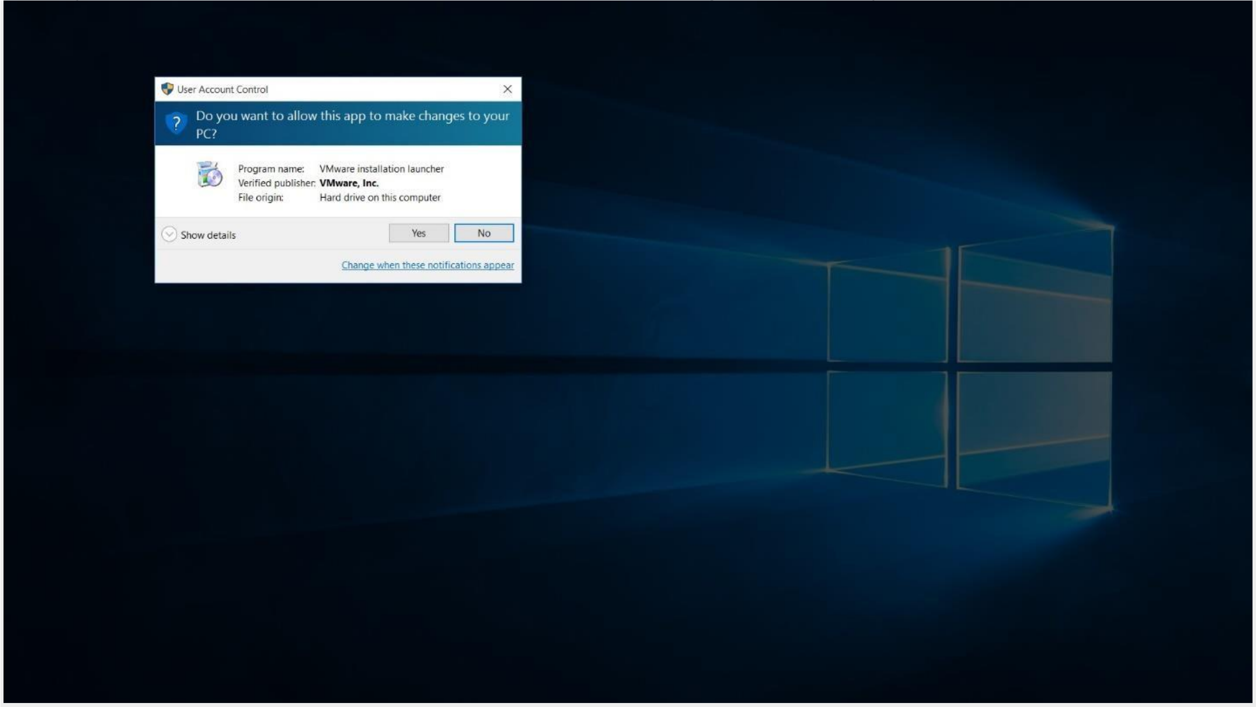
Step 3- Locate the downloaded installer file
For demonstration purpose, I have placed the downloaded installer on my desktop. Find the installer on your system and double click to launch the application.


Recycle Bin
Shailesh Jha
This PC
VMware-workstation-full-12.0.0-2985596
Search the web and Windows
11:53 PM
12/27/2015

VMware workstation 15 pro for windows 10 installer file screenshot.

Step 4- User Access Control (UAC) Warning

Now you should see User Access Control (UAC) dialog box. Click yes to continue.



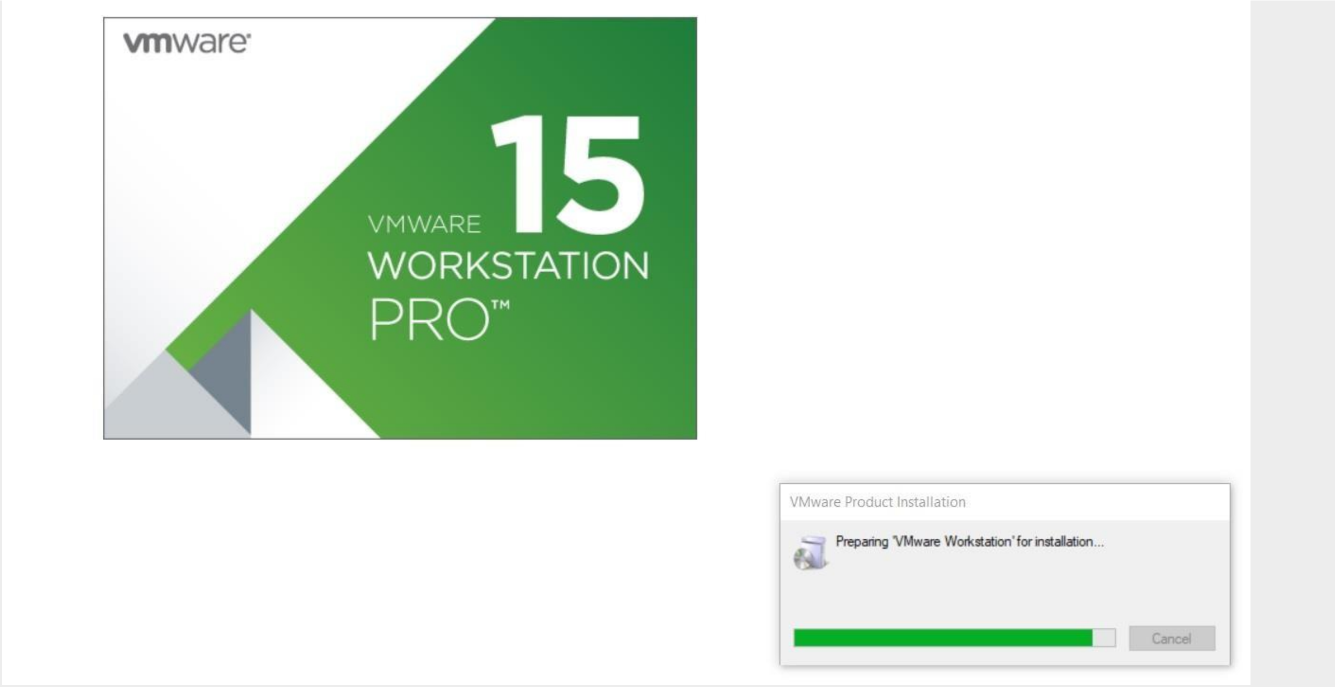
User Account Control

Do you want to allow this app to make changes to your PC?

Program name: VMware installation launcher
Verified publisher: **VMware, Inc.**
File origin: Hard drive on this computer

VMware Workstation 12 Pro installer windows 10 UAC screenshot

Initial Splash screen will appear. Wait for the process to complete.



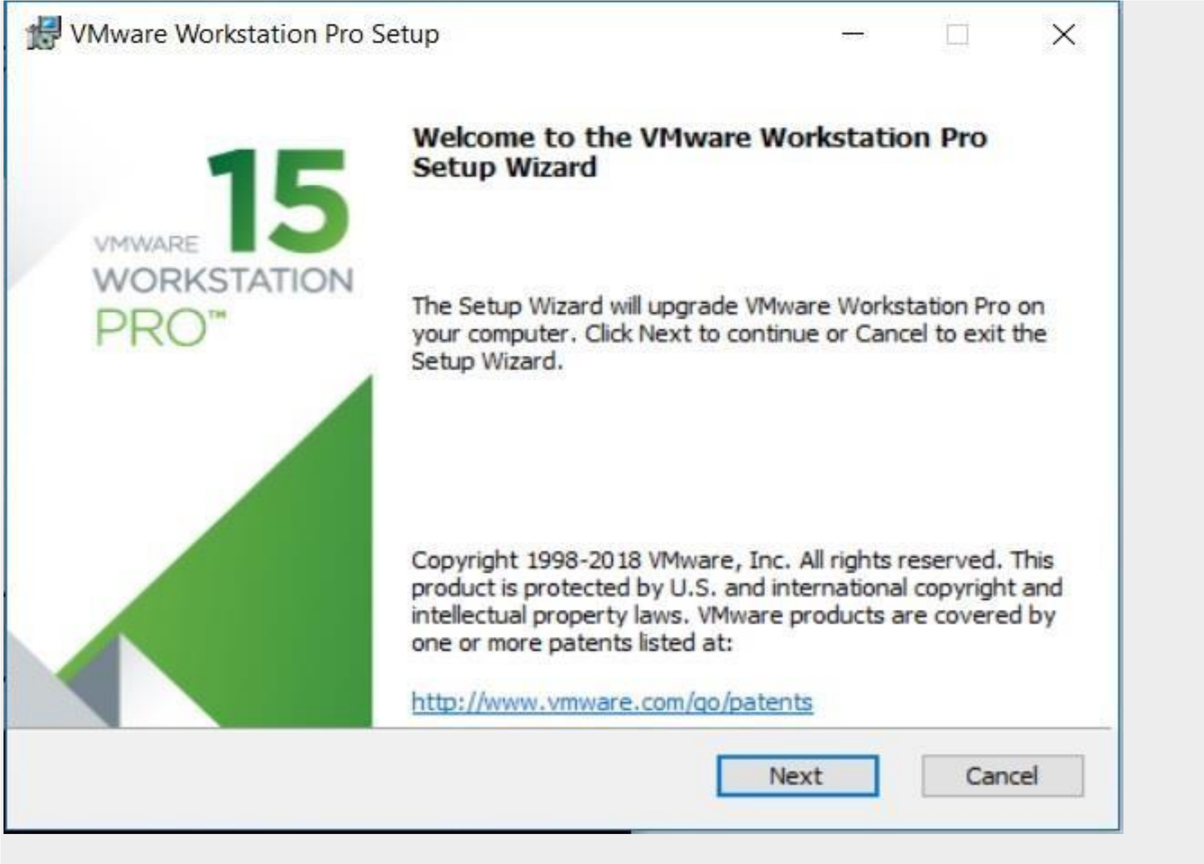
VMware Product Installation

Preparing 'VMware Workstation' for installation...

VMware Workstation 15 Installation Splash Screen

Step 5- VMware Workstation Setup wizard

Now you will see VMware Workstation setup wizard dialog box. Click next to continue.



VMware Workstation Pro Setup

Welcome to the VMware Workstation Pro Setup Wizard

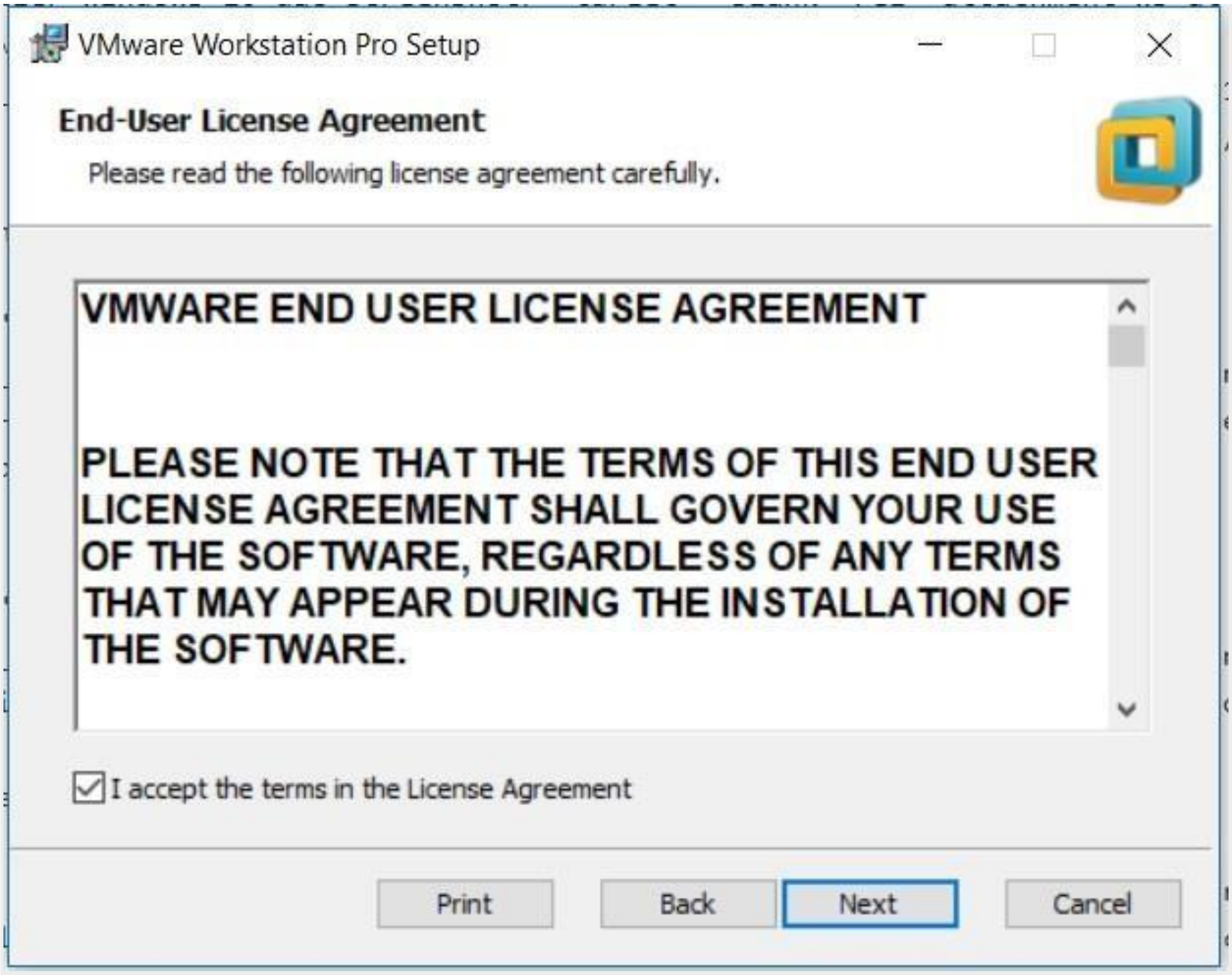
The Setup Wizard will upgrade VMware Workstation Pro on your computer. Click Next to continue or Cancel to exit the Setup Wizard.

Copyright 1998-2018 VMware, Inc. All rights reserved. This product is protected by U.S. and international copyright and intellectual property laws. VMware products are covered by one or more patents listed at:

http://www.vmware.com/go/patents

Step 6- End User Licence Agreement

This time you should see End User Licence Agreement dialog box. Check “I accept the terms in the Licence Agreement” box and press next to continue.



End-User License Agreement

Please read the following license agreement carefully.

VMWARE END USER LICENSE AGREEMENT

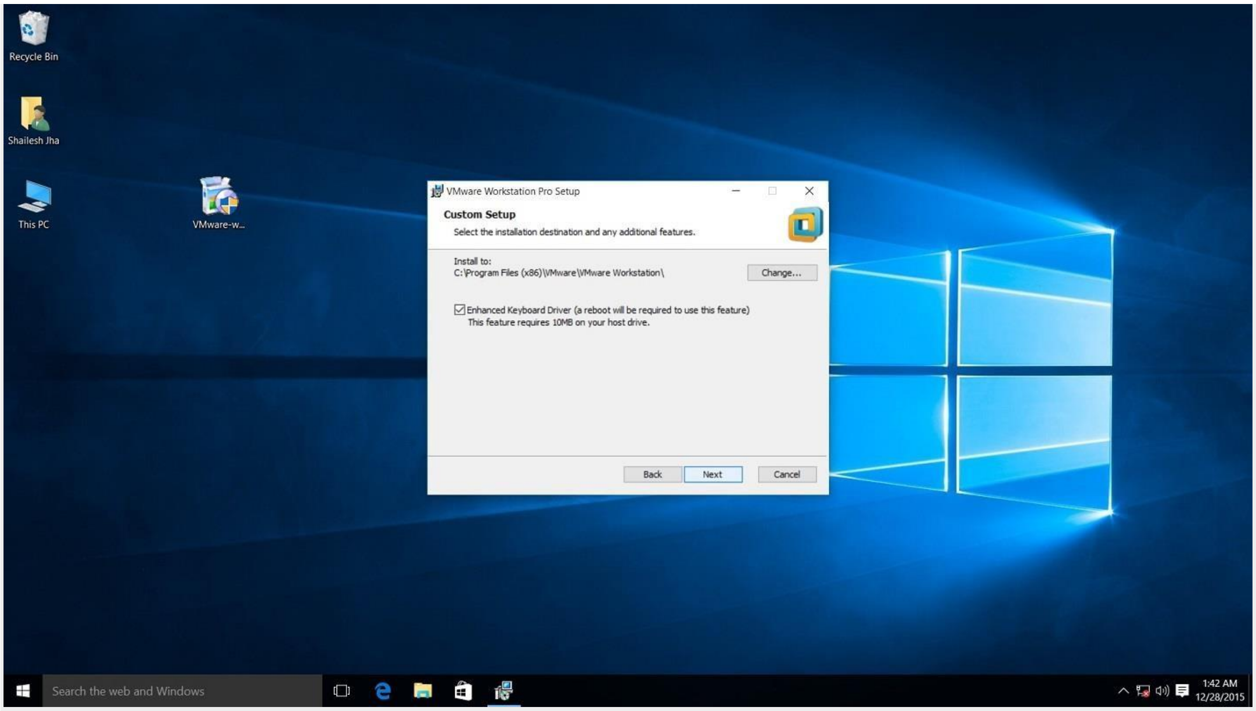
PLEASE NOTE THAT THE TERMS OF THIS END USER LICENSE AGREEMENT SHALL GOVERN YOUR USE OF THE SOFTWARE, REGARDLESS OF ANY TERMS THAT MAY APPEAR DURING THE INSTALLATION OF THE SOFTWARE.

☑ I accept the terms in the License Agreement

VMware Workstation 15 Installation – End User Licence Agreement

Step 7- Custom Setup options

Select the folder in which you would like to install the application. There is no harm in leaving the defaults as it is. Also select Enhanced Keyboard Driver check box.



VMware Workstation Pro Setup

Custom Setup

Select the installation destination and any additional features.

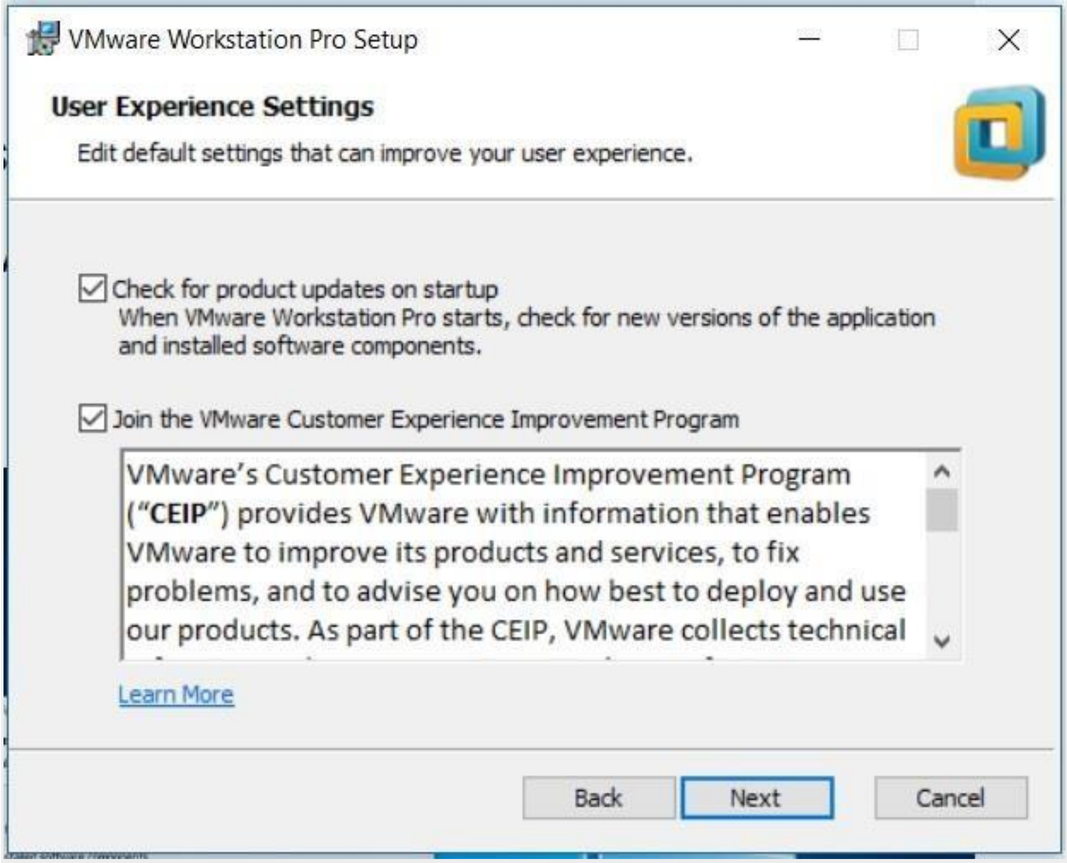
Install to:
C:\Program Files (x86)\VMware\VMware Workstation\

☑ Enhanced Keyboard Driver (a reboot will be required to use this feature)
This feature requires 10MB on your host drive.

VMware Workstation 15 Pro installation – select installation folder

Step 8- User Experience Settings

Next you are asked to select “Check for Updates” and “Help improve VMware Workstation Pro”. Do as you wish. I normally leave it to defaults that is unchecked.



VMware Workstation Pro Setup

User Experience Settings

Edit default settings that can improve your user experience.

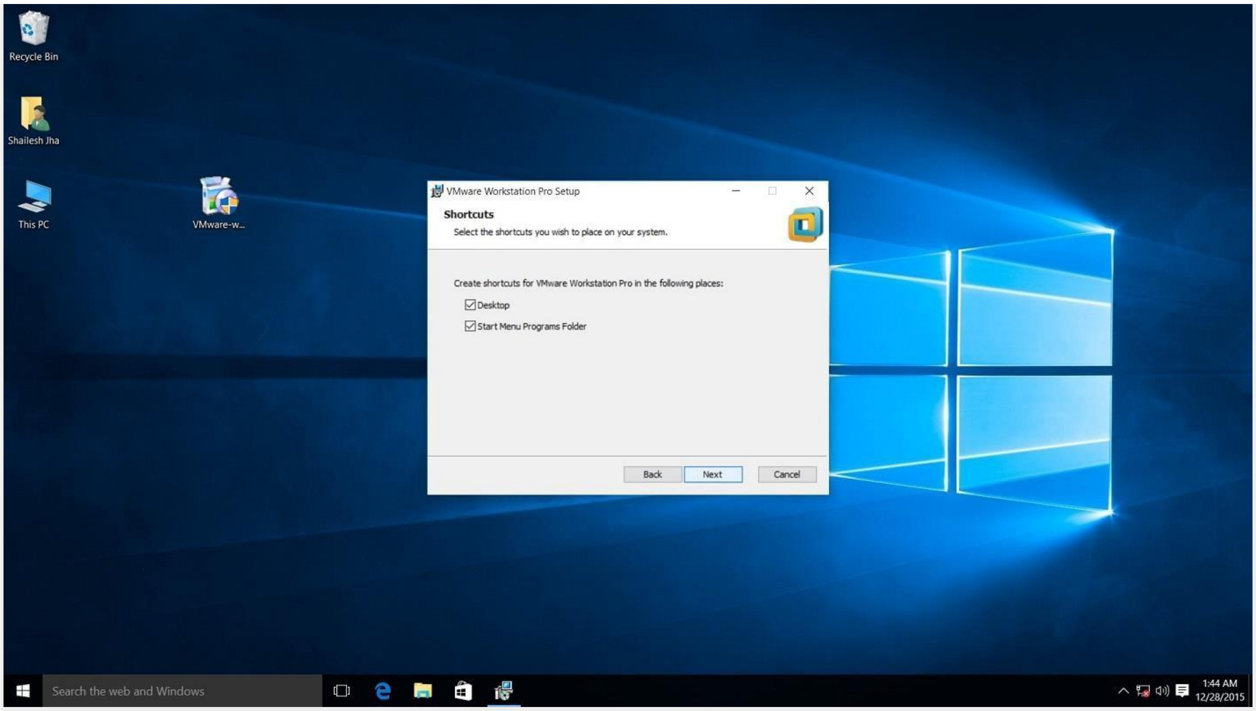
☑ Check for product updates on startup
When VMware Workstation Pro starts, check for new versions of the application and installed software components.

☑ Join the VMware Customer Experience Improvement Program

VMware’s Customer Experience Improvement Program (“CEIP”) provides VMware with information that enables VMware to improve its products and services, to fix problems, and to advise you on how best to deploy and use our products. As part of the CEIP, VMware collects technical

Step 9- Application Shortcuts preference

Next step is to select the place you want the shortcut icons to be placed on your system to launch the application. Please select both the options, desktop and start menu and click next.



VMware Workstation Pro Setup

Shortcuts

Select the shortcuts you wish to place on your system.

Create shortcuts for VMware Workstation Pro in the following places:

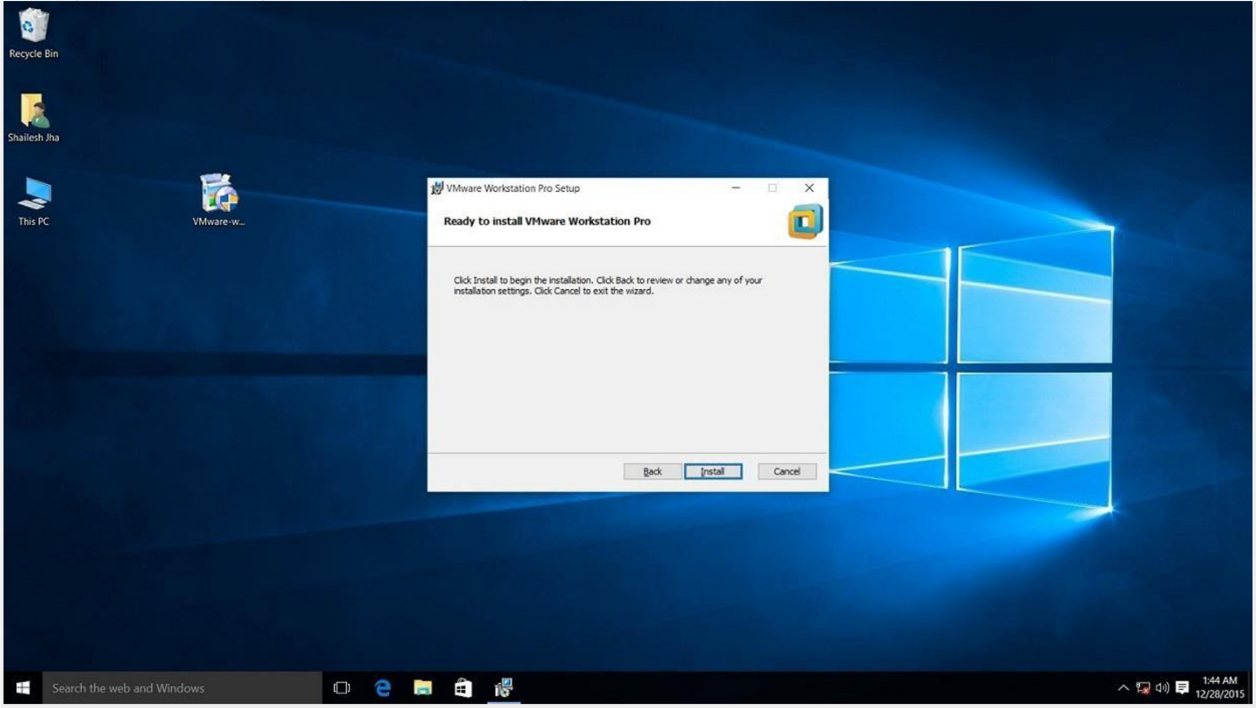
☑ Desktop

☑ Start Menu Programs Folder

VMware workstation 15 pro installation shortcut selection checkbox screenshot.

Step 10- Installation begins

Now you see the begin installation dialog box. Click install to start the installation process.



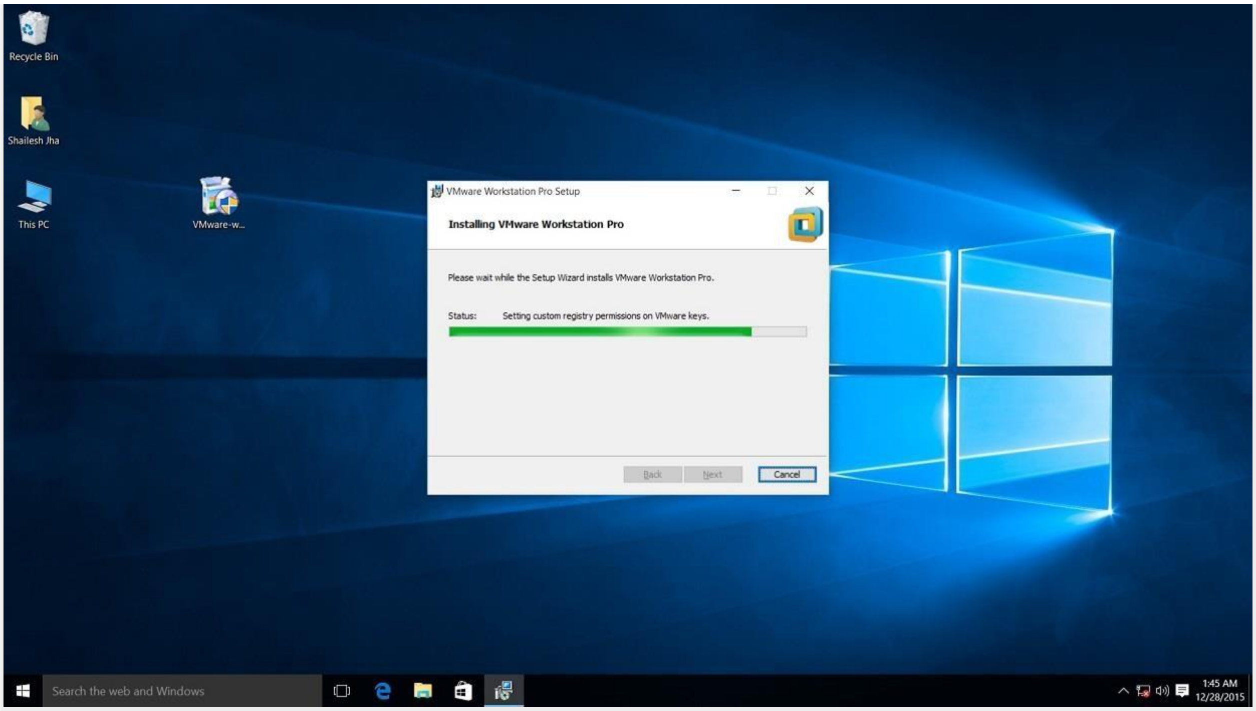
VMware Workstation Pro Setup

Ready to install VMware Workstation Pro

Click Install to begin the installation. Click Back to review or change any of your installation settings. Click Cancel to exit the wizard.

Screenshot for VMware Workstation 15 pro installation begin confirmation dialog box on windows 10.

Below screenshot shows Installation in progress. Wait for this to complete.



VMware Workstation Pro Setup

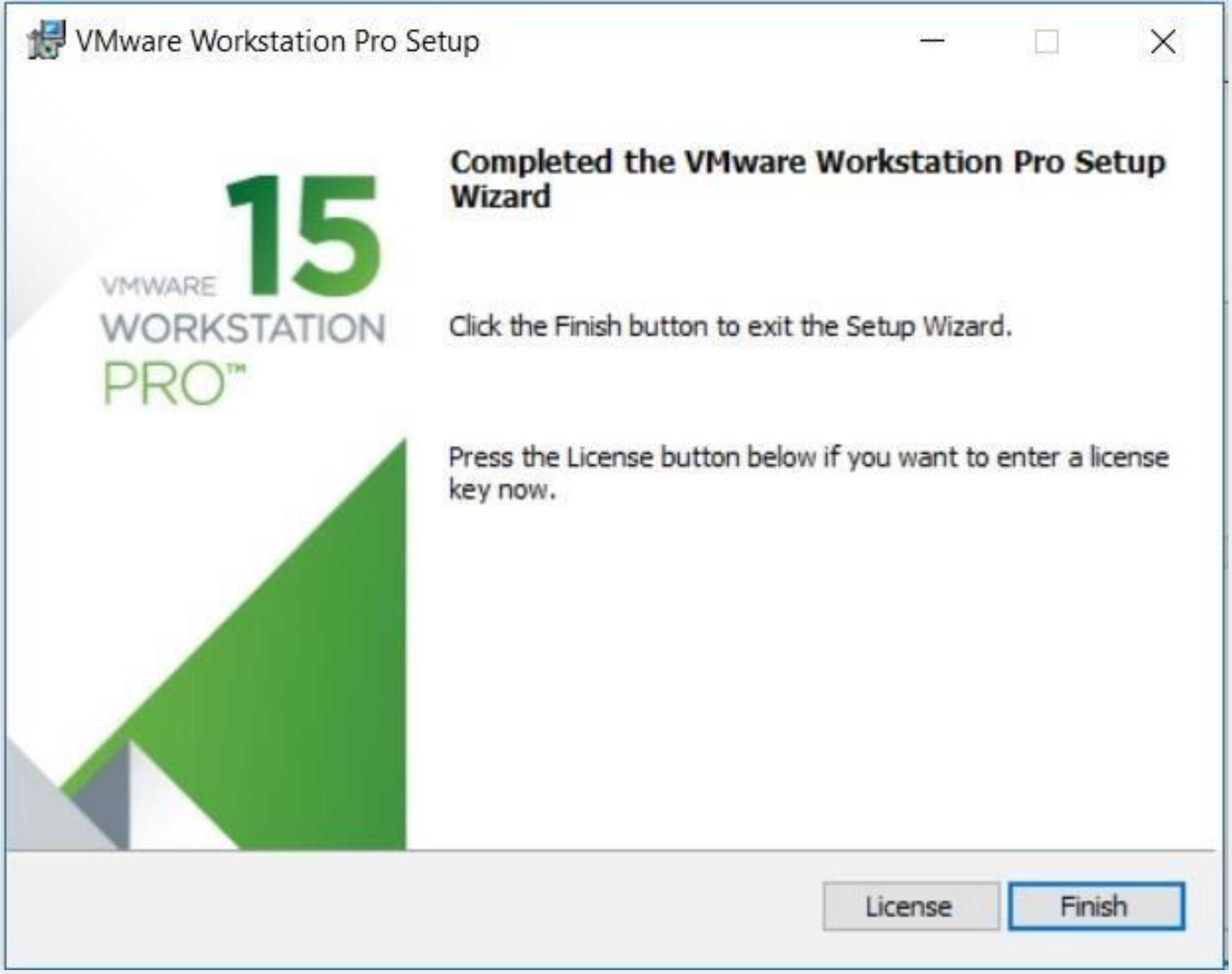
Installing VMware Workstation Pro

Please wait while the Setup Wizard installs VMware Workstation Pro.

Status: Setting custom registry permissions on VMware keys.

Screenshot for VMware Workstation 15 pro installation process.

At the end you will see installation complete dialog box. Click finish and you are done with the installation process. You may be asked to restart your computer. Click on Yes to restart.



VMware Workstation Pro Setup

Completed the VMware Workstation Pro Setup Wizard

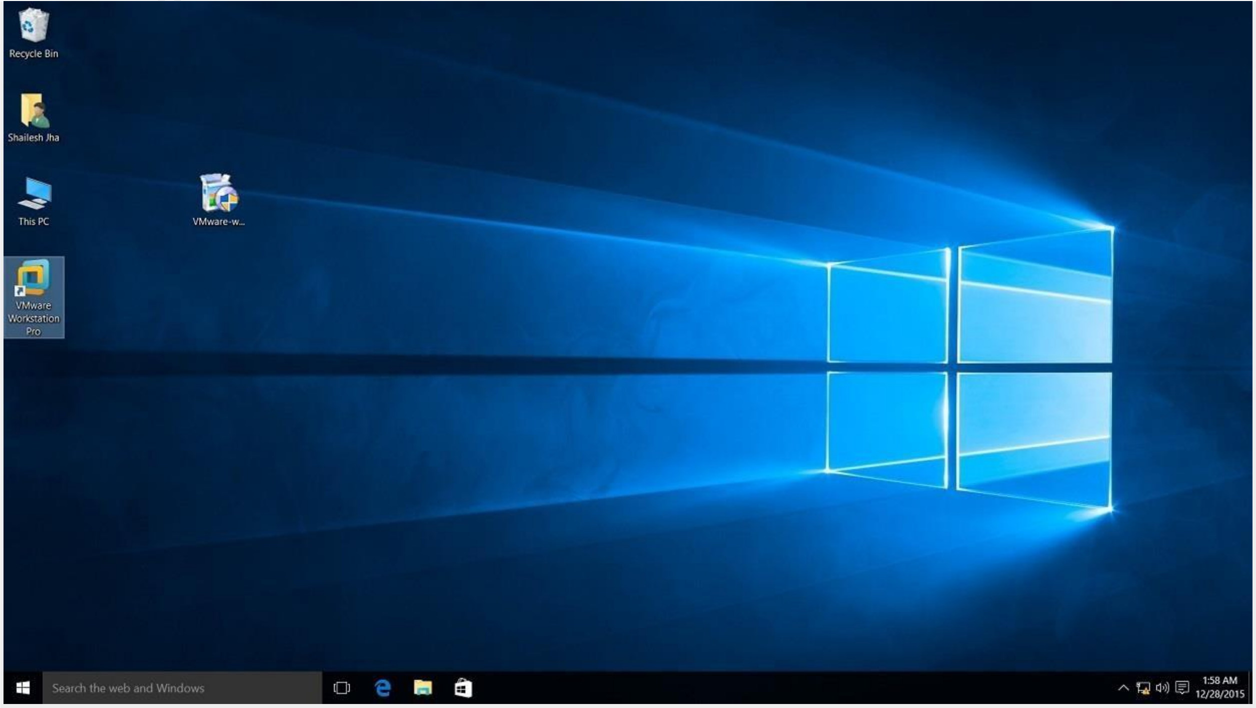
Click the Finish button to exit the Setup Wizard.

Press the License button below if you want to enter a license key now.

VMware Workstation 15 Installation – Installation Complete

Step 11- Launch VMware Workstation

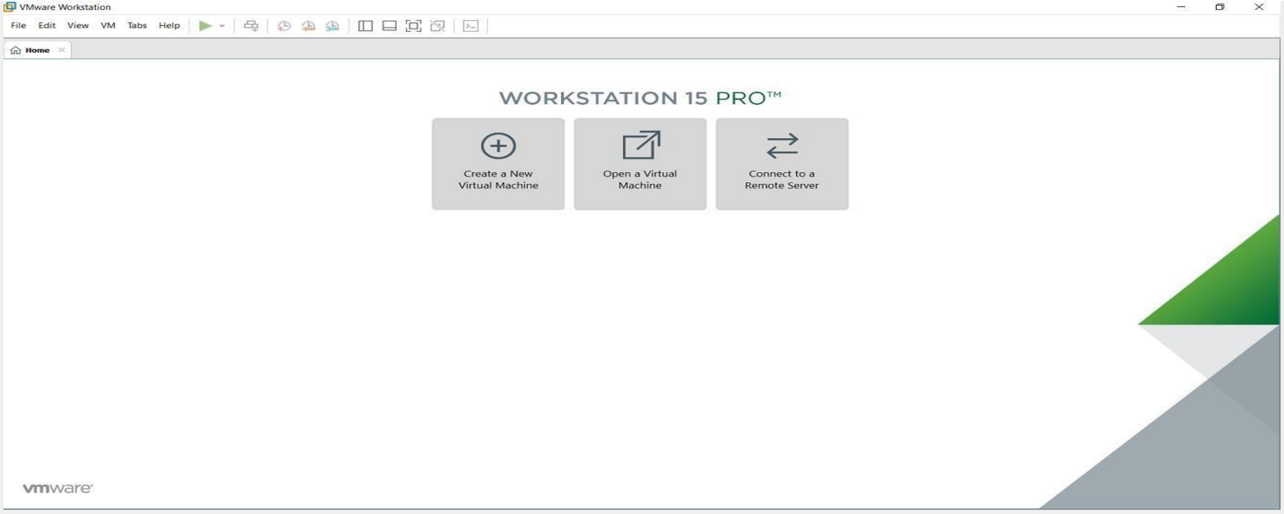
After the installation completes, you should see VMware Workstation icon on the desktop. Double clickon it to launch the application.



Screenshot for VMware Workstation 15 Pro icon on windows 10 desktop.

Step 12- Licence Key

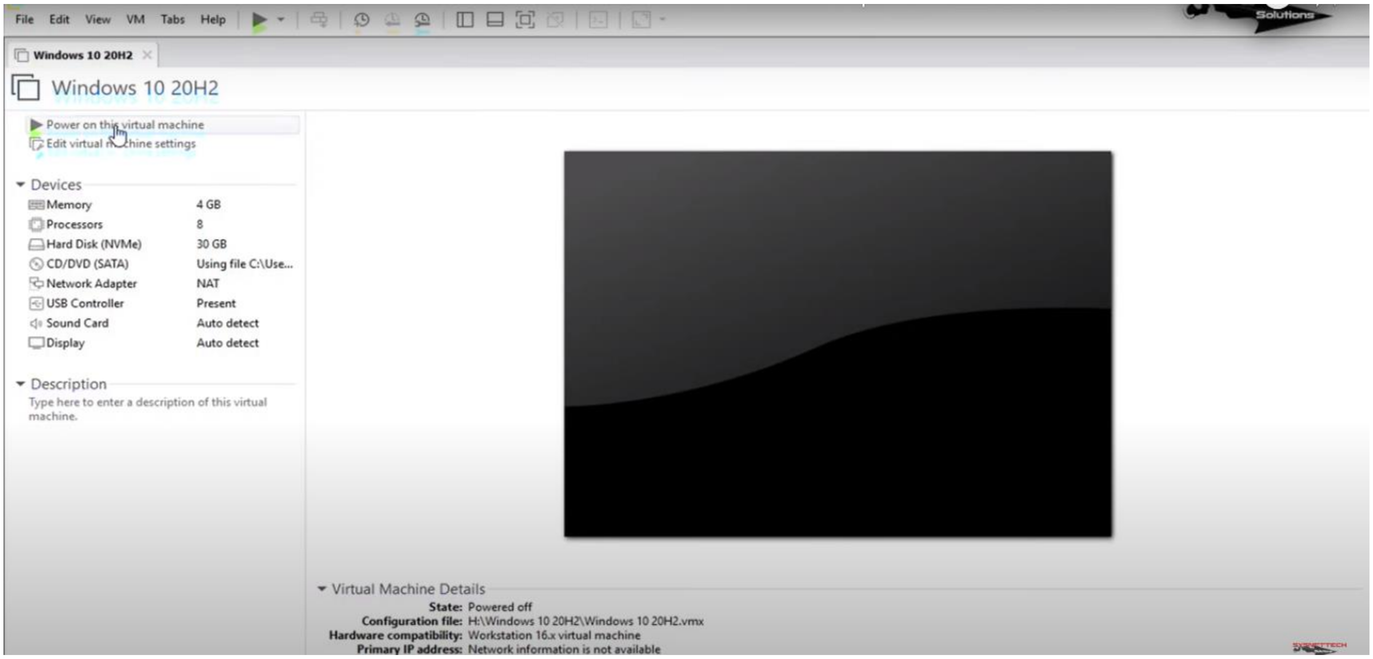
If you see the dialog box asking for licence key, click on trial or enter the licence key. Then what you have is the VMware Workstation 15 Pro running on your windows 10 desktop. If don’t have the licencekey, you will have 30 days trial.



VMware Workstation 15 Pro home screen

Step 13- At some point if you decide to buy

At some point of time if you decide to buy the Licence key, you can enter the Licence key by goingto **Help->Enter a Licence Key**You can enter the 25 character licence key in the dialog box shown below and click OK. Now you havethe licence version of the software.


File Edit View VM Tabs Help
Windows 10 20H2
Solutions
▶ Power on this virtual machine
Edit virtual machine settings

Windows 10 20H2

Devices

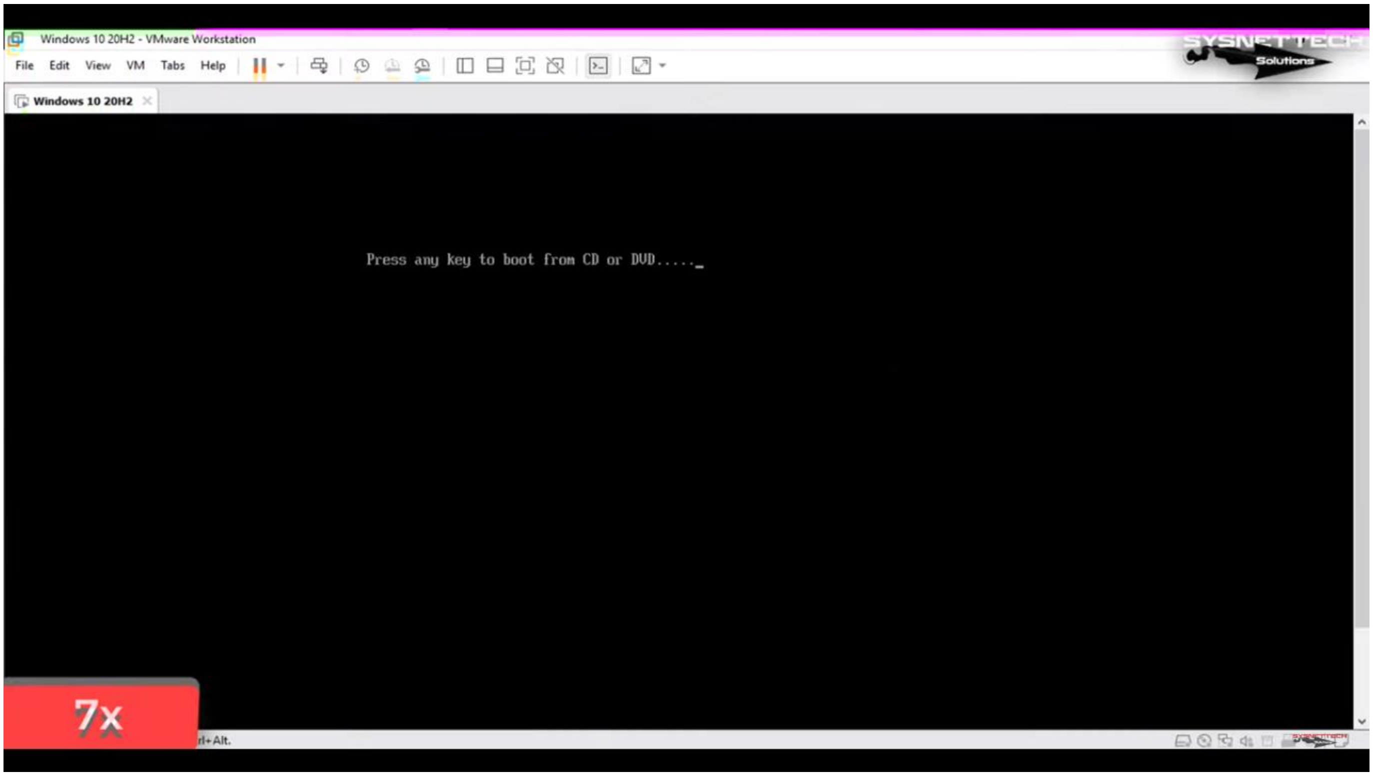
Memory	4 GB
Processors	8
Hard Disk (NVMe)	30 GB
CD/DVD (SATA)	Using file C:\Use...
Network Adapter	NAT
USB Controller	Present
Sound Card	Auto detect
Display	Auto detect

Description

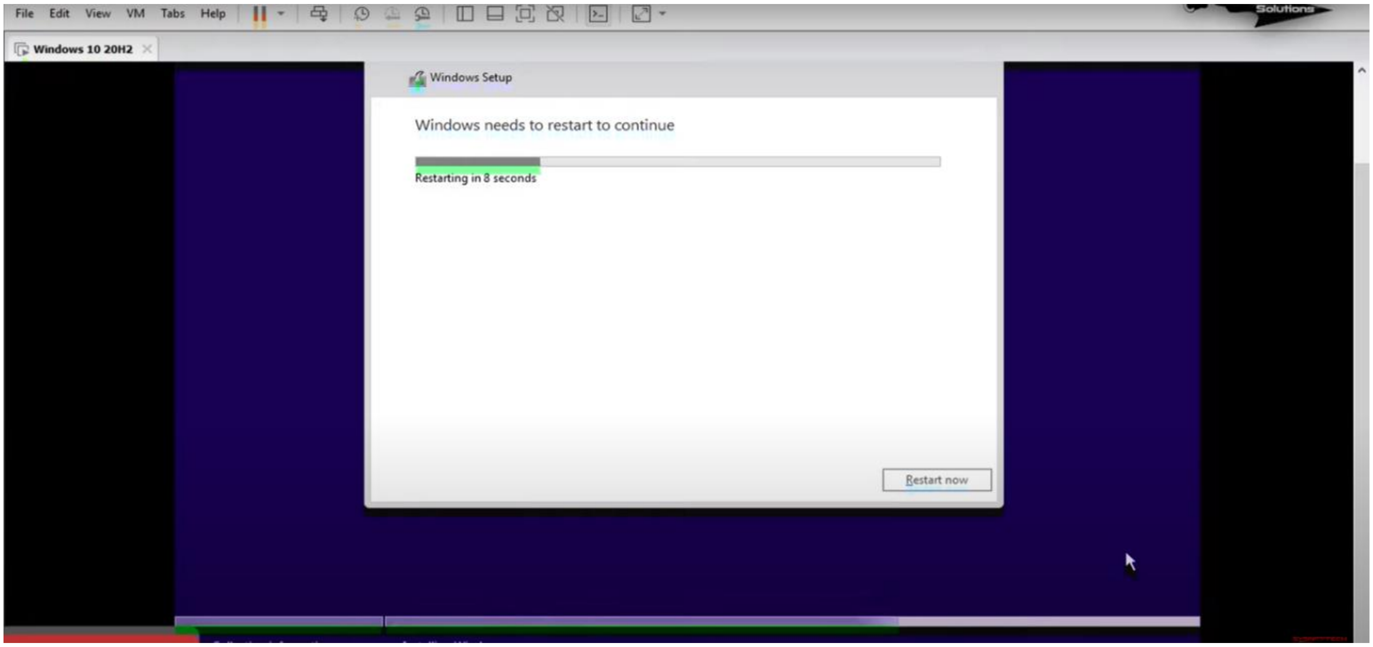
Type here to enter a description of this virtual machine.

Virtual Machine Details

State: Powered off
Configuration file: H:\Windows 10 20H2\Windows 10 20H2.vmx
Hardware compatibility: Workstation 16.x virtual machine
Primary IP address: Network information is not available

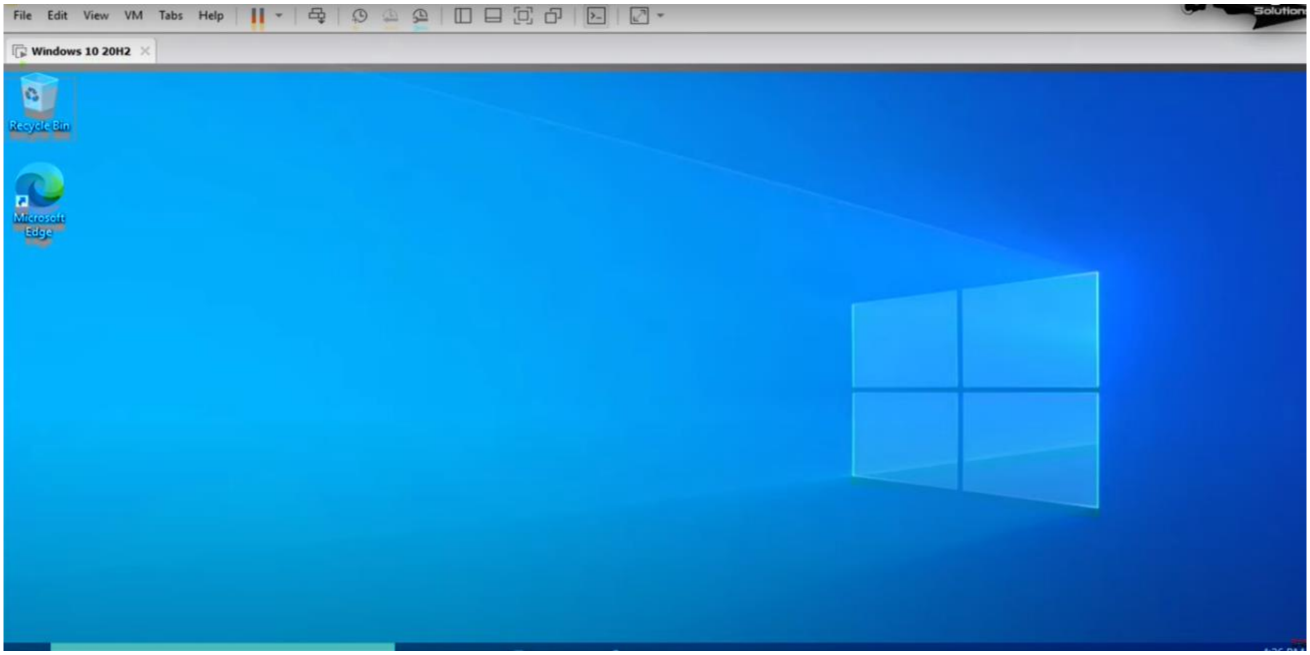

Windows 10 20H2 - VMware Workstation
File Edit View VM Tabs Help
Windows 10 20H2
SYSNETTECH
Solutions
7x
rl+Alt.

```
Press any key to boot from CD or DVD....._
```



Windows needs to restart to continue

Restarting in 8 seconds



RESULT:

EX.NO 2:

DATE :

INSTALL A C COMPILER IN THE VIRTUAL MACHINE AND EXECUTE A SAMPLE PROGRAM

AIM:
To Install a C compiler in the virtual machine and execute a sample C program.

PROCEDURE :
Step 1 : Open VMware software.
Step 2 : Create the virtual machine and startup the virtual machine.
Step 3: Install C compiler and type the following sample C program in Turbo c which is installed on virtual machine.

PROGRAM:

OUTPUT:

RESULT :

EX. NO 3:

DATE :

INSTALL GOOGLE APP ENGINE CREATE HELLO WORLD APP AND OTHER SIMPLE WEB APPLICATIONS USING PYTHON/JAVA.

AIM:

To create hello world app and other simple web applications using python/java.

ALGORITHM:

1. **Install Google cloud SDK and python softwares.**
2. **Authenticate the cloud SDK account by giving username and password.**
3. **Create python and yaml files in you directory.**
4. **Set the path in Google cloud shell and run the server.**
5. **Type http://localhost:8080 in the browser and the result will be displayed.**

PROGRAM:

OUTPUT:

RESULT :

EX. NO. 4

DATE:

USE GAE LAUNCHER TO LAUNCH THE WEB APPLICATIONS

AIM:

To launch GAE launcher to launch the web applications.

ALGORITHM:

1. **Install Google App Engine Software.**
2. **Create the application name and open the directory that you have created.**
3. **Create the yaml and python files in your directory.**
4. **Run the Google App Engine to launch the application.**

PROGRAM:

OUTPUT:

RESULT :

EX.NO 5:

DATE :

SIMULATE A CLOUD SCENARIO USING CLOUDSIM AND RUN A SCHEDULING ALGORITHM THAT IS NOT PRESENT IN CLOUDSIM

AIM : To simulate a cloud scenario using Cloud Sim and run a scheduling algorithm that is not present in Cloud Sim

PROCEDURE : The steps to be followed: How to use CloudSim in Eclipse
CloudSim is written in Java. The knowledge you need to use CloudSim is basic Java programming and some basics about cloud computing. Knowledge of programming IDEs such as Eclipse or NetBeans is also helpful. It is a library and, hence, CloudSim does not have to be installed. Normally, you can unpack the downloaded package in any directory, add it to the Javaclasspath and it is ready to be used. Please verify whether Java is available on your system.

To use CloudSim in Eclipse:

1. Download CloudSim installable files from ***https://code.google.com/p/cloudsim/downloads/list and unzip***
2. Open Eclipse
3. Create a new Java Project: File -> New
4. Import an unpacked CloudSim project into the new Java Project
5. The first step is to initialize the CloudSim package by initializing the CloudSim library, asfollows:
   CloudSim.init(num_user, calendar, trace_flag)

6. Data centre's are the resource providers in CloudSim; hence, creation of data centres is a second step. To create Datacenter, you need the DatacenterCharacteristics object that stores the properties of a data centre such as architecture, OS, list of machines, allocation policy that coversthe time or space shared, the time zone and its price:
   Datacenter datacenter9883 = new Datacenter(name, characteristics, new VmAllocationPolicySimple(hostList), s

7. The third step is to create a broker:
   DatacenterBroker broker = createBroker();

8. The fourth step is to create one virtual machine unique ID of the VM, userId ID of the VM'sowner, mips, number Of Pes amount of CPUs, amount of RAM, amount of bandwidth, amount of storage, virtual machine monitor, and cloudletScheduler policy for cloudlets:
   VM vm = new Vm(vmid, brokerId, mips, pesNumber, ram, bw, size, vmm, new CloudletSchedulerTimeShared())

9. Submit the VM list to the broker:
   broker.submitVmList(vmlist)

10. Create a cloudlet with length, file size, output size, and utilisation model:
    Cloudlet cloudlet = new Cloudlet(id, length, pesNumber, fileSize, outputSize, utilizationModel, utilizationMode
11. Submit the cloudlet list to the broker:

```
broker.submitCloudletList(cloudletList)
```

12. Start the simulation:

```
CloudSim.startSimulation()
```

Sample Output from the Existing Example:

```
Starting CloudSimExample1...Initialising...
Starting CloudSim version 3.0Datacenter_0 is starting...
>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>>null
Broker is starting...Entities started.
0.0: Broker: Cloud Resource List received with 1 resource(s)0.0: Broker: Trying to Create VM #0 in
Datacenter_0
0.1: Broker: VM #0 has been created in Datacenter #2, Host #0
0.1: Broker: Sending cloudlet 0 to VM #0
400.1: Broker: Cloudlet 0 received
400.1 : Broker: All Cloudlets executed. Finishing...400.1: Broker: Destroying VM #0
Broker is shutting down... Simulation: No more future events
CloudInformationService: Notify all CloudSim entities for shutting down.Datacenter_0 is shutting
down...
Broker is shutting down...Simulation completed.
Simulation completed.
```

PROGRAM:

OUTPUT:

RESULT :

EX.NO 6:

DATE :

FILES TRANSFER FROM ONE VIRTUAL MACHINE TO ANOTHER VIRTUAL MACHINE.

AIM : To find a procedure to transfer the files from one virtual machine to another virtual machine.

PROCEDURE :

1. You can copy few (or more) lines with ***copy & paste*** mechanism.
   For this you need to share clipboard between host OS and guest OS, installing **Guest Addition** on both the virtual machines (probably setting *bidirectional* and restarting them).You *copy* from *guest OS* in the clipboard that is shared with the *host OS*.
   Then you *paste* from the *host OS* to the second *guest OS*.
2. You can enable **drag and drop** too with the same method (Click on the machine, settings,general, advanced, drag and drop: set to *bidirectional*)
3. You can have **common *Shared Folders*** on both virtual machines and use one of thedirectory shared as buffer to copy.
   Installing **Guest Additions** you have the possibility to set Shared Folders too. As you put afile in a shared folder from *host OS* or from *guest OS*, is immediately visible to the other. (Keep in mind that can arise some problems for date/time of the files when there are different clock settings on the different virtual machines).
   If you use the same folder shared on more machines you can exchange files directly copyingthem in this folder.
4. You can use **usual method to copy files between 2 different computer** with client-serverapplication. (e.g. scp with sshd active for linux, winscp... you can get some info about SSHservers e.g. here)
   You need an active server (sshd) on the receiving machine and a client on the sending machine. Of course you need to have the authorization setted (via password or, better, viaan automatic authentication method).
   Note: many Linux/Ubuntu distribution install sshd by default: you can see if it is runningwith pgrep sshd from a shell. You can install with sudo apt-get install openssh-server.
5. You can **mount part of the file system** of a virtual machine via NFS or SSHFS on theother, or you can **share file and directory** with Samba.
   You may find interesting the article Sharing files between guest and host withoutVirtualBox shared folders with detailed step by step instructions.

You should remember that you are dialling with a little network of machines with differentoperative systems, and in particular:

- Each virtual machine has its own operative system running on and acts as a physicalmachine.
- Each virtual machine is an instance of a program *owned* by an *user* in the hosting operativesystem and should undergo the restrictions of the *user* in the *hosting OS*.
  E.g Let we say that Hastur and Meow are users of the hosting machine, but they did not allow each other to see their directories (no read/write/execute authorization). When each ofthem run a virtual machine, for the hosting OS those virtual machine are two normal programs owned by Hastur and Meow and cannot see the private directory of the other user.This is a restriction due to the *hosting OS*. It's easy to overcame it: it's enough to give authorization to read/write/execute to a directory or to chose a different directory in which both users can read/write/execute.
- Windows likes mouse and Linux fingers. :-)
  I mean I suggest you to enable *Drag & drop* to be cosy with the Windows machines andthe *Shared folders* or to be cosy with Linux.

When you will need to be fast with Linux **you will feel the need** of ssh-keygen an to Generate once SSH Keys to copy files on/from a remote machine without writingpassword anymore. In this way it functions \bash auto-completion remotely too!

PROGRAM:

OUTPUT:

RESULT :

EX.NO 7:

DATE :

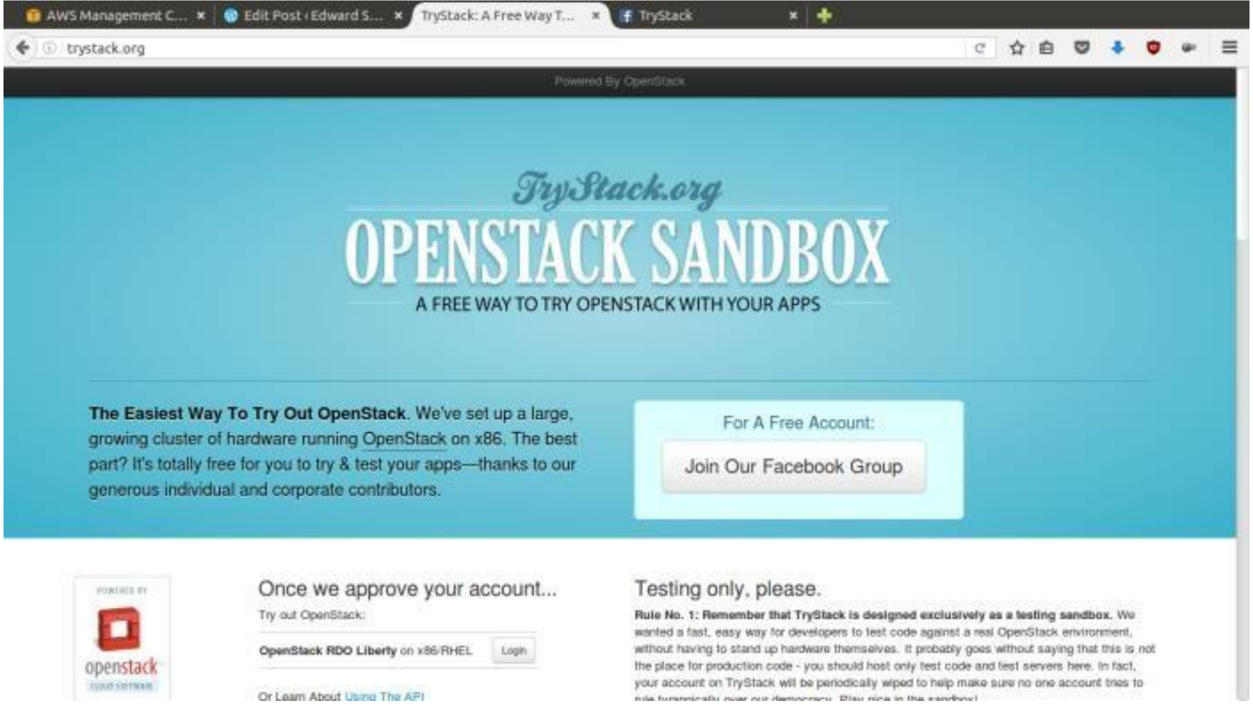
TO LAUNCH VIRTUAL MACHINE USING TRYSTACK

AIM : To find a procedure to launch virtual machine using trystack.

PROCEDURE :

OpenStack is an open-source software cloud computing platform. OpenStack is primarily used for deploying an infrastructure as a service (IaaS) solution like Amazon Web Service (AWS). Inother words, you can *make your own AWS* by using OpenStack. If you want to try out OpenStack, **TryStack** is the easiest and free way to do it.

In order to try OpenStack in TryStack, you must register yourself by joining TryStack Facebook Group. The acceptance of group needs a couple days because it's approved manually. After youhave been accepted in the TryStack Group, you can log in TryStack.



The Easiest Way To Try Out OpenStack. We've set up a large, growing cluster of hardware running OpenStack on x86. The best part? It's totally free for you to try & test your apps—thanks to our generous individual and corporate contributors.

Once we approve your account...

Try out OpenStack:

OpenStack RDO Liberty on x86/RHEL

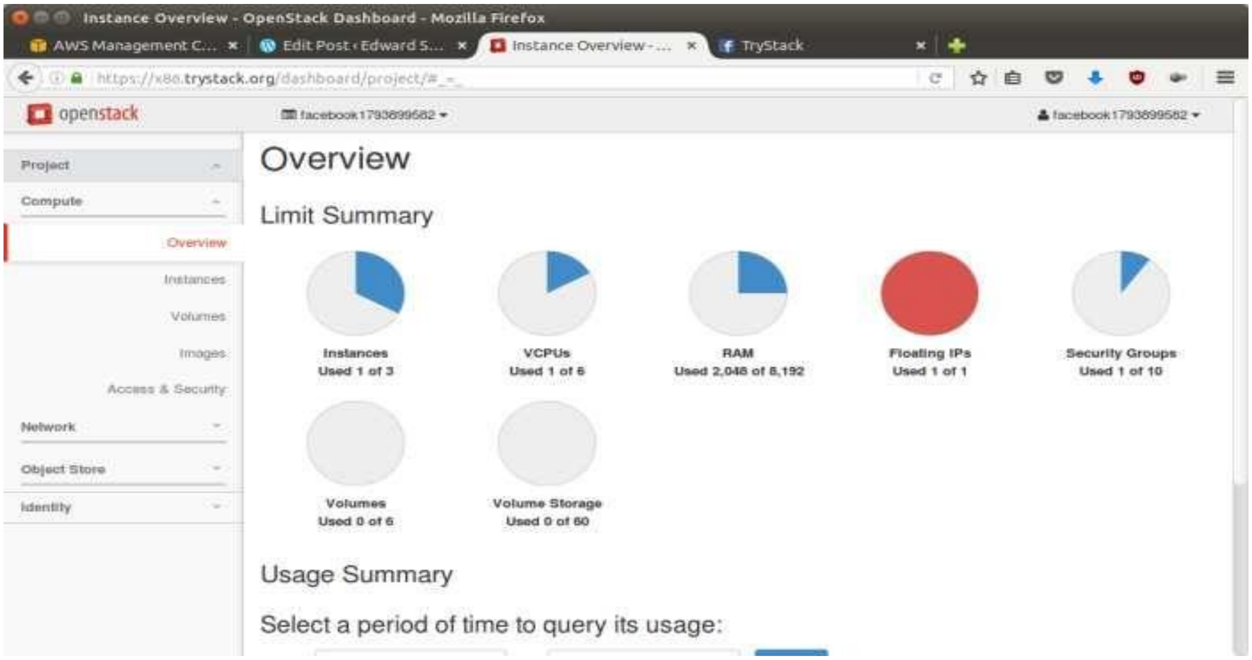
Or Learn About Using The API

Testing only, please.

Rule No. 1: Remember that TryStack is designed exclusively as a testing sandbox. We wanted a fast, easy way for developers to test code against a real OpenStack environment, without having to stand up hardware themselves. It probably goes without saying that this is not the place for production code - you should host only test code and test servers here. In fact, your account on TryStack will be periodically wiped to help make sure no one account tries to rule tyrannically over our democracy. Play nice in the sandbox!

TryStack.org Homepage

I assume that you already join to the Facebook Group and login to the dashboard. After you login to the TryStack, you will see the Compute Dashboard like:



Overview

Limit Summary

Instances	VCPUs	RAM	Floating IPs	Security Groups
Used 1 of 3	Used 1 of 6	Used 2,048 of 8,192	Used 1 of 1	Used 1 of 10

Volumes	Volume Storage
Used 0 of 6	Used 0 of 60

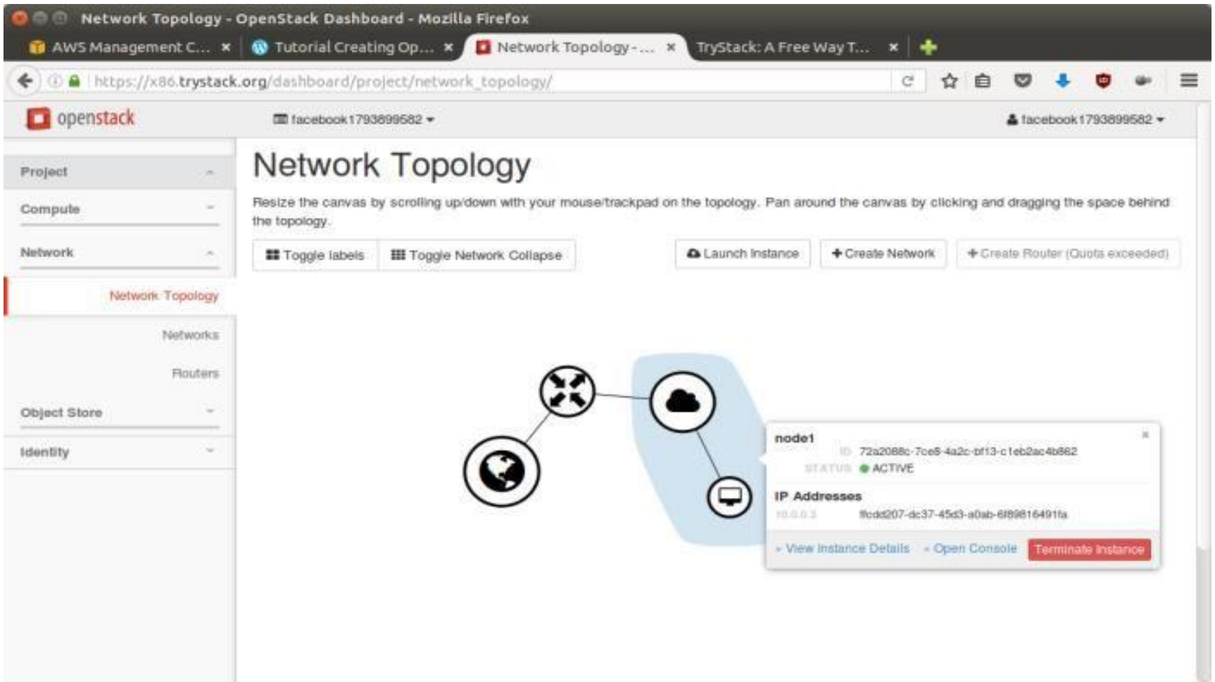
Usage Summary

Select a period of time to query its usage:

OpenStack Compute Dashboard

Run an OpenStack instance.

The instance will be accessiblethrough the internet (have a public IP address). The final topology will like:



Network Topology

Resize the canvas by scrolling up/down with your mouse/trackpad on the topology. Pan around the canvas by clicking and dragging the space behind the topology.

node1

ID 72a2088c-7ce8-4a2c-bf13-c1eb2ac4b862

STATUS ● ACTIVE

IP Addresses

10.0.0.3 ffcdd207-dc37-45d3-a0ab-6f89816491fa

Network topology

As you see from the image above, the instance will be connected to a local network and the localnetwork will be connected to internet.

Step 1: Create Network

Network? Yes, the network in here is our own local network. So, your instances will be not mixed up with the others. You can imagine this as your own LAN (Local Area Network) in the cloud.

1. Go to **Network > Networks** and then click **Create Network**.
2. In **Network** tab, fill **Network Name** for example internal and then click **Next**.
3. In **Subnet** tab,
   1. Fill **Network Address** with appropriate CIDR, for example 192.168.1.0/24. Use privatenetwork CIDR block as the best practice.
   2. Select **IP Version** with appropriate IP version, in this case IPv4.
   3. Click **Next**.
4. In **Subnet Details** tab, fill **DNS Name Servers** with 8.8.8.8 (Google DNS) and thenclick **Create**.

Step 2: Create Instance

Now, we will create an instance. The instance is a virtual machine in the cloud, like AWS EC2. You need the instance to connect to the network that we just created in the previous step.

1. Go to **Compute > Instances** and then click **Launch Instance**.
2. In **Details** tab,
   1. Fill **Instance Name**, for example Ubuntu 1.
   2. Select **Flavor**, for example m1.medium.
   3. Fill **Instance Count** with **1**.
   4. Select **Instance Boot Source** with **Boot from Image**.
   5. Select **Image Name** with **Ubuntu 14.04 amd64 (243.7 MB)** if you want install Ubuntu 14.04 in your virtual machine.
3. In **Access & Security** tab,
   1. Click [+] button of **Key Pair** to import key pair. This key pair is a public and private key thatwe will use to connect to the instance from our machine.
   2. In **Import Key Pair** dialog,
      1. Fill **Key Pair Name** with your machine name (for example Edward-Key).
      2. Fill **Public Key** with your **SSH public key** (usually is in ~/.ssh/id_rsa.pub). Seedescription in Import Key Pair dialog box for more information. If you are usingWindows, you can use **Puttygen** to generate key pair.
      3. Click **Import key pair**.
   3. In **Security Groups**, mark/check **default**.
4. In **Networking** tab,
   1. In **Selected Networks**, select network that have been created in Step 1, for example internal.
5. Click **Launch**.
6. If you want to create multiple instances, you can repeat step 1-5. I created one more instancewith instance name Ubuntu 2.

Step 3: Create Router In the step 1, we created our network, but it is isolated.It doesn’t connect to the internet. To make our network has an internet connection, we need a router that running as the gateway to the internet.

1. Go to **Network > Routers** and then click **Create Router**.
2. Fill **Router Name** for example router1 and then click **Create router**.
3. Click on your **router name link**, for example router1, **Router Details** page.
4. Click **Set Gateway** button in upper right:
    1. Select **External networks** with **external**.
    2. Then **OK**.
5. Click **Add Interface** button.
    1. Select **Subnet** with the network that you have been created in Step 1.
    2. Click **Add interface**.
6. Go to **Network > Network Topology**. You will see the network topology. In the example, thereare two network, i.e. external and internal, those are bridged by a router. There are instances those are joined to internal network.

Step 4: Configure Floating IP Address

Floating IP address is public IP address. It makes your instance is accessible from the internet. When you launch your instance, the instance will have a private network IP, but no public IP. In OpenStack, the public IPs is collected in a pool and managed by admin (in our case is TryStack). You need to request a public (floating) IP address to be assigned to your instance.

1. Go to **Compute > Instance**.
2. In one of your instances, click **More > Associate Floating IP**.
3. In **IP Address**, click Plus [**+**].
4. Select **Pool** to **external** and then click **Allocate IP**.
5. Click **Associate**.
6. Now you will get a public IP, e.g. 8.21.28.120, for your instance.

Step 5: Configure Access & Security

OpenStack has a feature like a firewall. It can whitelist/blacklist your in/out connection. It iscalled *Security Group*.

1. Go to **Compute > Access & Security** and then open **Security Groups** tab.
2. In **default** row, click **Manage Rules**.
3. Click **Add Rule**, choose **ALL ICMP** rule to enable ping into your instance, and then click **Add**.
4. Click **Add Rule**, choose **HTTP** rule to open HTTP port (port 80), and then click **Add**.
5. Click **Add Rule**, choose **SSH** rule to open SSH port (port 22), and then click **Add**.
6. You can open other ports by creating new rules.

Step 6: SSH to Your Instance

Now, you can SSH your instances to the floating IP address that you got in the step 4. If you areusing Ubuntu image, the SSH user will be ubuntu.

OUTPUT:

RESULT :

EX.NO 8:

DATE :

INSTALL HADOOP SINGLE NODE CLUSTER AND RUNSIMPLE APPLICATIONS LIKE WORDCOUNT

AIM :

To install hadoop single node cluster and run simple applications like wordcount.

PROCEDURE:

1. Hardware Requirement
   * RAM — Min. 8GB, if you have SSD in your system then 4GB RAM would also work.
   * CPU — Min. Quad core, with at least 1.80GHz
2. JRE 1.8 — Offline installer for JRE
3. Java Development Kit — 1.8
4. A Software for Un-Zipping like 7Zip or Win Rar
5. Download Hadoop zip

2. Unzip and Install Hadoop

After Downloading the Hadoop, we need to Unzip the hadoop-3.5.5.tar.gz file.

Now we can organize our Hadoop installation, we can create a folder and move the final extracted file in it.

Please note while creating folders, DO NOT ADD SPACES IN BETWEEN THE FOLDER NAME

3. Setting Up Environment Variables

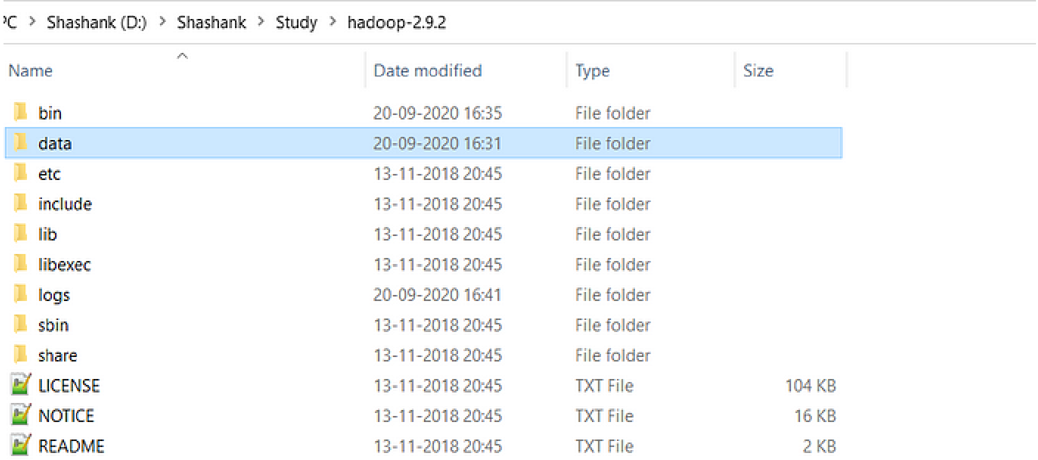
Another important step in setting up a work environment is to set your Systems environment variable.

To edit environment variables, go to Control Panel > System > click on the “Advanced system settings” link
Alternatively, We can Right click on This PC icon and click on Properties and click on the “Advanced system settings” link Or, easiest way is to search for Environment Variable in search bar and there you go

INSTALLATION PROCEDURE:

Editing Hadoop files

Once we have configured the environment variables next step is to configure Hadoop. It has 3 parts:-



ᐟC > Shashank (D:) > Shashank > Study > hadoop-2.9.2

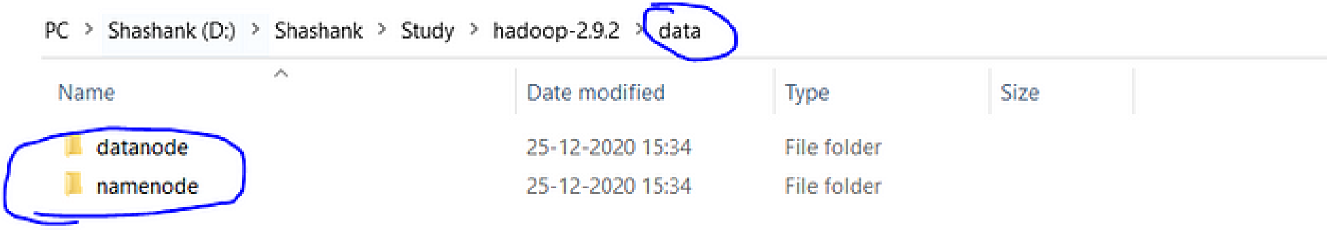
Name	Date modified	Type	Size
bin	20-09-2020 16:35	File folder	
data	20-09-2020 16:31	File folder	
etc	13-11-2018 20:45	File folder	
include	13-11-2018 20:45	File folder	
lib	13-11-2018 20:45	File folder	
libexec	13-11-2018 20:45	File folder	
logs	20-09-2020 16:41	File folder	
sbin	13-11-2018 20:45	File folder	
share	13-11-2018 20:45	File folder	
LICENSE	13-11-2018 20:45	TXT File	104 KB
NOTICE	13-11-2018 20:45	TXT File	16 KB
README	13-11-2018 20:45	TXT File	2 KB

Creating Folders

We need to create a folder data in the hadoop directory, and 2 sub folders namenode and datanode

Creating Data Folder

- Create **DATA folder** in the Hadoop directory



PC > Shashank (D:) > Shashank > Study > hadoop-2.9.2 > data

Name	Date modified	Type	Size
datanode	25-12-2020 15:34	File folder	
namenode	25-12-2020 15:34	File folder	

Creating Sub-folders

- Once DATA folder is created, we need to create 2 new folders namely, **namenode and datanode** inside the data folder
- These folders are important because files on HDFS resides inside the datanode.

Editing Configuration Files

Now we need to edit the following config files in hadoop for configuring it :-
(We can find these files in Hadoop -> etc -> hadoop)
* core-site.xml
* hdfs-site.xml
* mapred-site.xml
* yarn-site.xml
* hadoop-env.cmd

Editing core-site.xml

Right click on the file, select edit and paste the following content within <configuration> </configuration> tags.

Note:- Below part already has the configuration tag, we need to copy only the part inside it.

```
<configuration>
<property>
  <name>fs.defaultFS</name>
  <value>hdfs://localhost:9000</value>
 </property>
</configuration>
```

Editing hdfs-site.xml

Right click on the file, select edit and paste the following content within <configuration></configuration>tags.

Note:- Below part already has the configuration tag, we need to copy only the part inside it. Also replace PATH~1 and PATH~2 with the path of namenode and datanode folder that we created recently(step 4.1).

```
<configuration>
 <property>
  <name>dfs.replication</name>
  <value>1</value>
 </property>
 <property>
  <name>dfs.namenode.name.dir</name>
  <value>PATH~1\namenode</value>
  <final>true</final>

</property>
 <property>
  <name>dfs.datanode.data.dir</name>
  <value>PATH~2\datanode</value>
  <final>true</final>
 </property>
</configuration>
```

Editing mapred-site.xml

Right click on the file, select edit and paste the following content within <configuration> </configuration> tags.

Note:- Below part already has the configuration tag, we need to copy only the part inside it.

```
<configuration>
 <property>
  <name>mapreduce.framework.name</name>
  <value>yarn</value>
 </property>
</configuration>
```

Editing yarn-site.xml

Right click on the file, select edit and paste the following content within <configuration> </configuration> tags.

Note:- Below part already has the configuration tag, we need to copy only the part inside it.

```
<configuration>
 <property>
  <name>yarn.nodemanager.aux-services</name>
  <value>mapreduce_shuffle</value>
 </property>
 <property>
  <name>yarn.nodemanager.auxservices.mapreduce.shuffle.class</name>
  <value>org.apache.hadoop.mapred.ShuffleHandler</value>


</property>
<!-- Site specific YARN configuration properties --></configuration>
```

Verifying hadoop-env.cmd

Right click on the file, select edit and check if the JAVA_HOME is set correctly or not.
We can replace the JAVA_HOME variable in the file with your actual JAVA_HOME that we configured in the System Variable.

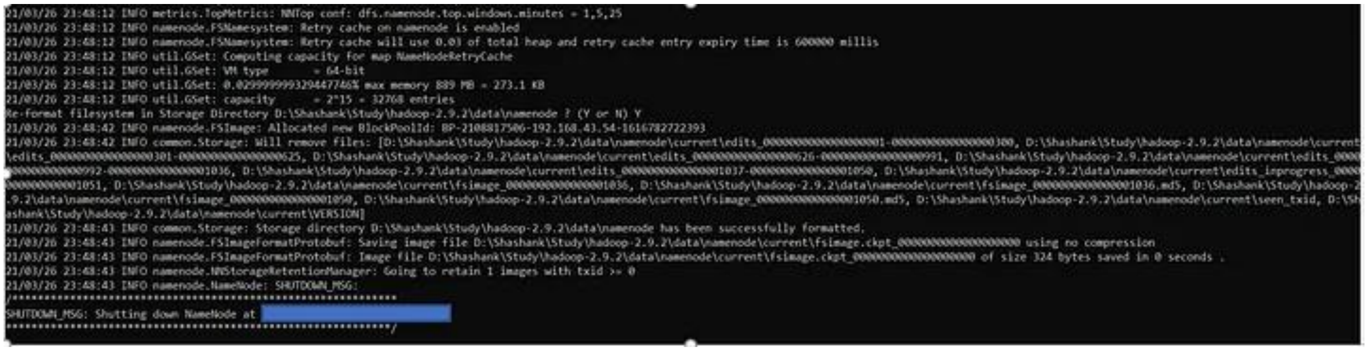
```
set JAVA_HOME=%JAVA_HOME%
         OR
set JAVA_HOME="C:\Program Files\Java\jdk1.8.0_221"
```

Replacing bin

Last step in configuring the hadoop is to download and replace the bin folder.
* Go to this GitHub Repo and download the bin folder as a zip.
* Extract the zip and copy all the files present under bin folder to %HADOOP_HOME%\bin

Formatting Namenode

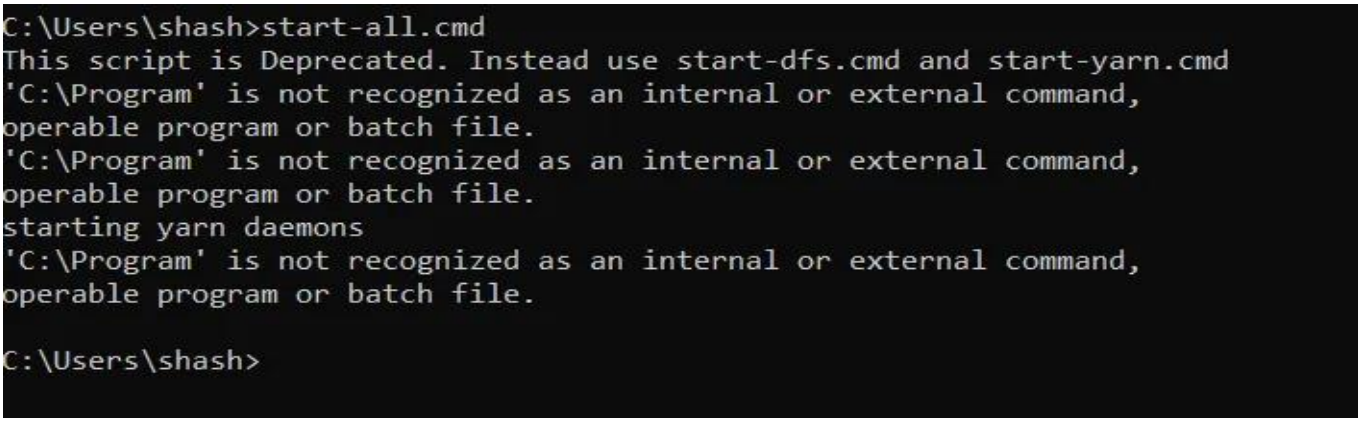
```
hadoop namenode -format
```



```
21/03/26 23:48:12 INFO metrics.TopMetrics: NNTop conf: dfs.namenode.top.windows.minutes = 1,5,25
21/03/26 23:48:12 INFO namenode.FSNamesystem: Retry cache on namenode is enabled
21/03/26 23:48:12 INFO namenode.FSNamesystem: Retry cache will use 0.03 of total heap and retry cache entry expiry time is 600000 millis
21/03/26 23:48:12 INFO util.GSet: Computing capacity for map NameNodeRetryCache
21/03/26 23:48:12 INFO util.GSet: VM type       = 64-bit
21/03/26 23:48:12 INFO util.GSet: 0.029999999329447746% max memory 889 MB = 273.1 KB
21/03/26 23:48:12 INFO util.GSet: capacity      = 2^15 = 32768 entries
Re-format filesystem in Storage Directory D:\Shashank\Study\hadoop-2.9.2\data\namenode ? (Y or N) Y
21/03/26 23:48:42 INFO namenode.FSImage: Allocated new BlockPoolId: BP-2108817506-192.168.43.54-1616782722393
21/03/26 23:48:42 INFO common.Storage: Will remove files: [D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\edits_0000000000000000001-0000000000000000300, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current
\edits_0000000000000000301-0000000000000000625, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\edits_0000000000000000626-0000000000000000991, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\edits_0000
0000000000000000992-0000000000000001036, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\edits_0000000000000001037-0000000000000001050, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\edits_inprogress_0000
0000000000000001051, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\fsimage_0000000000000001036, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\fsimage_0000000000000001036.md5, D:\Shashank\Study\hadoop-2
.9.2\data\namenode\current\fsimage_0000000000000001050, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\fsimage_0000000000000001050.md5, D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\seen_txid, D:\Sh
ashank\Study\hadoop-2.9.2\data\namenode\current\VERSION]
21/03/26 23:48:43 INFO common.Storage: Storage directory D:\Shashank\Study\hadoop-2.9.2\data\namenode has been successfully formatted.
21/03/26 23:48:43 INFO namenode.FSImageFormatProtobuf: Saving image file D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\fsimage.ckpt_0000000000000000000 using no compression
21/03/26 23:48:43 INFO namenode.FSImageFormatProtobuf: Image file D:\Shashank\Study\hadoop-2.9.2\data\namenode\current\fsimage.ckpt_0000000000000000000 of size 324 bytes saved in 0 seconds .
21/03/26 23:48:43 INFO namenode.NNStorageRetentionManager: Going to retain 1 images with txid >= 0
21/03/26 23:48:43 INFO namenode.NameNode: SHUTDOWN_MSG:
/************************************************************
SHUTDOWN_MSG: Shutting down NameNode at [redacted]
************************************************************/
```

Launching Hadoop

`start-all.cmd`

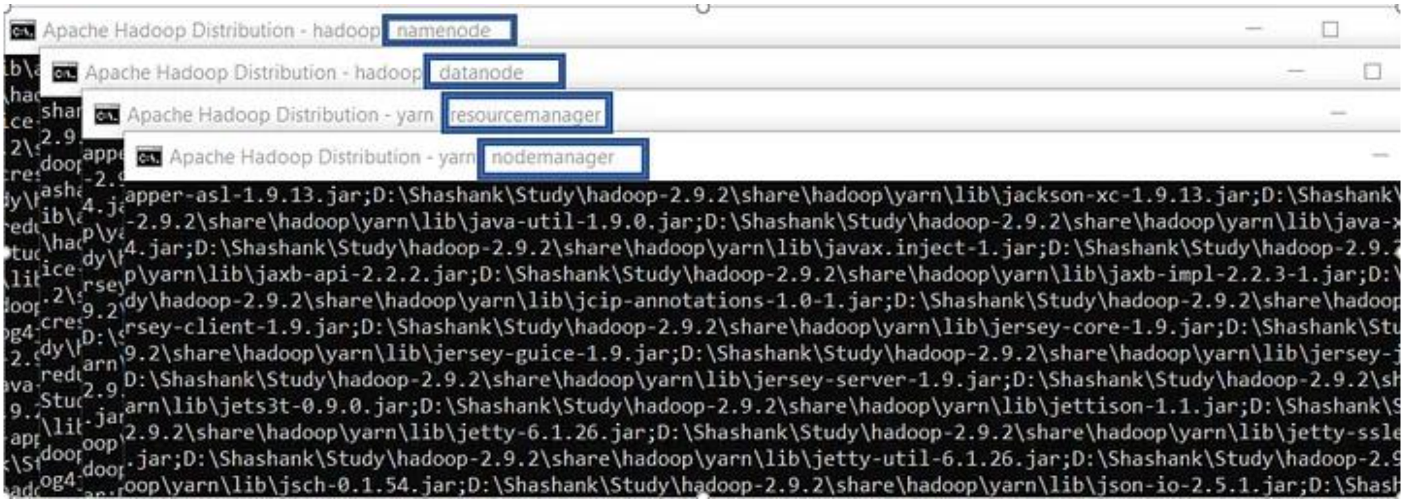


```
C:\Users\shash>start-all.cmd
This script is Deprecated. Instead use start-dfs.cmd and start-yarn.cmd
'C:\Program' is not recognized as an internal or external command,
operable program or batch file.
'C:\Program' is not recognized as an internal or external command,
operable program or batch file.
starting yarn daemons
'C:\Program' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\shash>
```

This will open 4 new cmd windows running 4 different Daemons of hadoop:-

* Namenode
* Datanode
* Resourcemanager
* Nodemanager


Apache Hadoop Distribution - hadoop namenode
Apache Hadoop Distribution - hadoop datanode
Apache Hadoop Distribution - yarn resourcemanager
Apache Hadoop Distribution - yarn nodemanager

```
apper-asl-1.9.13.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jackson-xc-1.9.13.jar;D:\Shashank\
-2.9.2\share\hadoop\yarn\lib\java-util-1.9.0.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\java-x
4.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\javax.inject-1.jar;D:\Shashank\Study\hadoop-2.9.2
p\yarn\lib\jaxb-api-2.2.2.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jaxb-impl-2.2.3-1.jar;D:\
dy\hadoop-2.9.2\share\hadoop\yarn\lib\jcip-annotations-1.0-1.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop
rsey-client-1.9.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jersey-core-1.9.jar;D:\Shashank\Stu
9.2\share\hadoop\yarn\lib\jersey-guice-1.9.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jersey-j
D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jersey-server-1.9.jar;D:\Shashank\Study\hadoop-2.9.2\sh
arn\lib\jets3t-0.9.0.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jettison-1.1.jar;D:\Shashank\S
2.9.2\share\hadoop\yarn\lib\jetty-6.1.26.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jetty-ssle
.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\jetty-util-6.1.26.jar;D:\Shashank\Study\hadoop-2.9
oop\yarn\lib\jsch-0.1.54.jar;D:\Shashank\Study\hadoop-2.9.2\share\hadoop\yarn\lib\json-io-2.5.1.jar;D:\Shash
```

OUTPUT:

RESULT :

MADHA ENGINEERING COLLEGE

(Affiliated to Anna University and Approved by AICTE, New Delhi)
Madha Nagar, Kundrathur, Chennai-600069

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

COMMON TO: DEPARTMENT OF INFORMATION TECHNOLOGY

IT8761– SECURITY LABORATORY

R 2017

LAB MANUAL

INDEX

Ex.No. : 1a **CAESAR CIPHER**
Date :

AIM:

To implement a Caesar cipher substitution technique in Java.

ALGORITHM:

1. Assign the 26 letters in alphabet to the variable named ALPHABET.
2. Convert the plaintext letters into lowercase.
3. To encrypt a plaintext letter, the first set of plaintext letters and slides it to LEFT by the number of positions of the secret shift.
4. The plaintext letter is then encrypted to the ciphertext letter on the sliding ruler underneath.
5. On receiving the ciphertext, the receiver who also knows the secret shift, positions his sliding ruler underneath the ciphertext alphabet and slides it to RIGHT by the agreed shift number, 3 in this case.
6. Then replaces the ciphertext letter by the plaintext letter on the sliding ruler underneath.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 1b **PLAYFAIR CIPHER**
Date :

AIM:

To implement a Playfair cipher substitution technique in Java.

ALGORITHM:

1. Read the keyword.
2. Then create the key table of 5x5 grid of alphabets.
3. Read the word to encrypt.
4. Ifthe input word should be even and then process it.
5. Then the plaintext message is split into pairs of two letters (digraphs).
6. Ifboth the letters are in the same column, take the letter below each one.
7. Ifboth letters are in the same row, take the letter to the right of each one.
8. If neither of the preceding two rules are true, form a rectangle with the two letters and take the letters on the horizontal opposite corner of the rectangle.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 1c **HILL CIPHER**

Date :

AIM:

To implement a Hill cipher substitution technique in Java.

ALGORITHM:

1. Obtain a plaintext message to encode in standard English with no spaces.
2. Split the plaintext into group of length three. To fill this, add X at the end.
3. Convert each group of letters with length three into plaintext vectors.
4. Replace each letter by the number corresponding to its position in the alphabet i.e. A=1, B=2, C=3…*Z*=0.
5. Create the keyword in a 3*3 matrix.
6. Multiply the two matrices to obtain the cipher text of length three.
7. For decryption, convert each entry in the ciphertext vector into its plaintext vector by multiplying the cipher text vector and inverse of a matrix.
8. Thus plain text is obtained fromcorresponding plaintext vector by corresponding position in the alphabet.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 1d **VIGENERE CIPHER**
Date :

AIM:

To implement a Java program for encryption and decryption using Vigenere cipher substitution technique.

ALGORITHM:

1. The Vigenere cipher is a method of encrypting alphabetic text by using a series of different Caesar ciphers based on the letters of a keyword.
2. It is a simple form of *polyalphabetic* substitution.
3. To encrypt, a table ofalphabets can be used, termed a Vigenere square, or Vigenere table.
4. It consists of the alphabet written out 26 times in different rows, each alphabet shifted cyclically to the left compared to the previous alphabet, corresponding to the 26 possible Caesar ciphers.
5. At different points in the encryption process, the cipher uses a different alphabet from one of the rows used.
6. The alphabet at each point depends on a repeating keyword.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 2a **RAIL FENCE CIPHER**

Date :

AIM:

To implement a rail fence transposition technique in Java.

ALGORITHM :

1. In the rail fence cipher, the plaintext is written downwards and diagonally on successive "rails" of an imaginary fence, then moving up when we reach the bottom rail.
2. When we reach the top rail, the message is written downwards again until the whole plaintext is written out.
3. The message is then read off in rows.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 2b ROW AND COLUMN TRANSFORMATION TECHNIQUE
Date :

AIM:

To implement a rail fence transposition technique in Java.

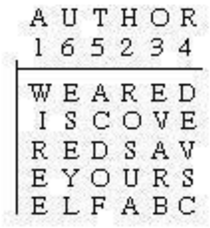
ALGORITHM:

1. Consider the plain text hello world, and let us apply the simple columnar transposition technique as shown below

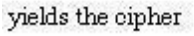
h	e	l	l
o	w	o	r
l	d		

2. The plain text characters are placed horizontally and the cipher text is created with vertical format as: **holewdlo lr**.
3. Now, the receiver has to use the same table to decrypt the cipher text to plain text.

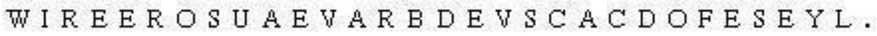
EXAMPLE:



A	U	T	H	O	R
1	6	5	2	3	4
W	E	A	R	E	D
I	S	C	O	V	E
R	E	D	S	A	V
E	Y	O	U	R	S
E	L	F	A	B	C



yields the cipher



W I R E E R O S U A E V A R B D E V S C A C D O F E S E Y L .

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 3 **DATA ENCRYPTION STANDARD (DES)**
Date :

AIM:

To apply Data Encryption Standard (DES) Algorithm for a practical application like User Message Encryption.

ALGORITHM:

1. Create a DES Key.
2. Create a Cipher instance from Cipher class, specify the following information and separated by a slash (/).
   - Algorithm name
   - Mode (optional)
   - Padding scheme (optional)
3. Convert String into Byte[] array format.
4. Make Cipher in encrypt mode, and encrypt it with Cipher.doFinal() method.
5. Make Cipher in decrypt mode, and decrypt it with Cipher.doFinal() method.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 4 **AES ALGORITHM**

Date :

AIM:

To apply Advanced Encryption Standard (AES) Algorithm for a practical application like URL Encryption.

ALGORITHM:

1. AES is based on a design principle known as a substitution–permutation.
2. AES does not use a Feistel network like DES, it uses variant of Rijndael.
3. It has a fixed block size of 128 bits, and a key size of 128, 192, or 256 bits.
4. AES operates on a 4 × 4 column- major order array of bytes, termed the state

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 5 **RSA ALGORITHM**

Date :

AIM:

To implement a RSA algorithm using HTML and Javascript.

ALGORITHM:

1. Choose two prime number p and q.
2. Compute the value of n and t.
3. Find the value of public key e.
4. Compute the value of private key d.
5. Do the encryption and decryption
    a. Encryption is given as,
        $c = t^e \bmod n$
    b. Decryption is given as,
        $t = c^d \bmod n$

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 6 **DIFFIE-HELLMAN KEY EXCHANGE ALGORITHM**
Date :

AIM:

To implement a Diffie-Hellman Key Exchange algorithm.

ALGORITHM:

1. Sender and receiver publicly agree to use a modulus *p* and base *g* which is a primitive root modulo p.
2. Sender chooses a secret integer x then sends Bob R1 = g^x mod *p*
3. Receiver chooses a secret integer y, then sends Alice R2 = g^y mod *p*
4. Sender computes k1 = B^x mod *p*
5. Receiver computes k2 = A^y mod *p*
6. Sender and Receiver now share a secret key.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 7 **SHA-1 ALGORITHM**

Date :

AIM:

To calculate the message digest of a text using the SHA-1 algorithm in Java.

ALGORITHM:

1. Append Padding bits.
2. Append Length - 64 bits are appended to the end.
3. Prepare Processing Functions.
4. Prepare Processing Constants.
5. Initialize Buffers.
6. Processing Message in 512-bit blocks (L blocks in total message).

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 8 **DIGITAL SIGNATURE SCHEME**
Date :

AIM:

To implement the signature scheme - Digital Signature Standard.

ALGORITHM:

1. Declare the class and required variables.
2. Create the object for the class in the main program.
3. Access the member functions using the objects.
4. Implement the SIGNATURE SCHEME - Digital Signature Standard.
5. It uses a hash function.
6. The hash code is provided as input to a signature function along with a random number K generated for the particular signature.
7. The signature function also depends on the sender,,s private key.
8. The signature consists of two components.
9. The hash code of the incoming message is generated.
10. The hash code and signature are given as input to a verification function.

PROGRAM:

OUTPUT:

RESULT:

Ex. No. : 9 **INTRUSION DETECTION SYSTEM (IDS)**
Date:

AIM:

To demonstrate Intrusion Detection System (IDS) using Snort software tool.

STEPS ON CONFIGURING AND INTRUSION DETECTION:

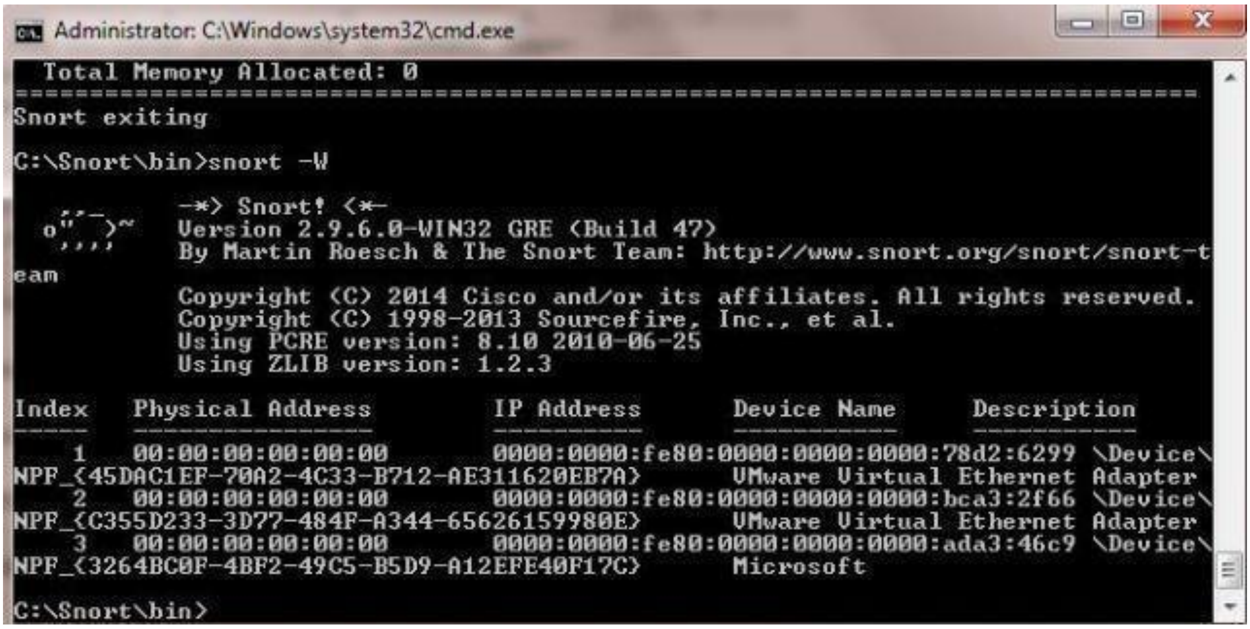
1. Download Snort from the Snort.org website. (http://www.snort.org/snort-downloads)
2. Download Rules(https://www.snort.org/snort-rules). You must register to get the rules. (You should download these often)
3. Double click on the .exe to install snort. This will install snort in the "C:\Snort" folder.It is important to have WinPcap (https://www.winpcap.org/install/) installed
4. Extract the Rules file. You will need WinRAR for the .gz file.
5. Copy all files from the "rules" folder of the extracted folder. Now paste the rules into *"C:\Snort\rules"* folder.
6. Copy "snort.conf" file from the "etc" folder of the extracted folder. You must paste it into "C:\Snort\etc" folder. Overwrite any existing file. Remember if you modify your snort.conf file and download a new file, you must modify it for Snort to work.
7. Open a command prompt (cmd.exe) and navigate to folder "C:\Snort\bin" folder. (at the Prompt, type cd\snort\bin)
8. To start (execute) snort in sniffer mode use following command:

```
snort -dev -i 3
```

-i indicates the interface number. You must pick the correct interface number. In my case, it is 3.
-dev is used to run snort to capture packets on your network.

To check the interface list, use following command:

```
snort -W
```



```
 Total Memory Allocated: 0
===============================================================================
Snort exiting

C:\Snort\bin>snort -W

   ,,_     -*> Snort! <*-
  o"  )~   Version 2.9.6.0-WIN32 GRE (Build 47)
   ''''    By Martin Roesch & The Snort Team: http://www.snort.org/snort/snort-t
eam
           Copyright (C) 2014 Cisco and/or its affiliates. All rights reserved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using PCRE version: 8.10 2010-06-25
           Using ZLIB version: 1.2.3

Index   Physical Address        IP Address      Device Name     Description
-----   -----------------       ----------      -----------     -----------
    1   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:78d2:6299 \Device\
NPF_{45DAC1EF-70A2-4C33-B712-AE311620EB7A}      VMware Virtual Ethernet Adapter
    2   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:bca3:2f66 \Device\
NPF_{C355D233-3D77-484F-A344-65626159980E}      VMware Virtual Ethernet Adapter
    3   00:00:00:00:00:00       0000:0000:fe80:0000:0000:0000:ada3:46c9 \Device\
NPF_{3264BC0F-4BF2-49C5-B5D9-A12EFE40F17C}      Microsoft

C:\Snort\bin>
```

Finding an interface

You can tell which interface to use by looking at the Index number and finding Microsoft. As you can see in the above example, the other interfaces are for VMWare. My interface is 3.

9. To run snort in IDS mode, you will need to configure the file “snort.conf” according to your network environment.
10. To specify the network address that you want to protect in snort.conf file, look for the following line.
var HOME_NET 192.168.1.0/24 (You will normally see any here)
11. You may also want to set the addresses of DNS_SERVERS, if you have some on your network.

Example:

example snort
12. Change the RULE_PATH variable to the path of rules folder.
var RULE_PATH c:\snort\rules

path to rules
13. Change the path of all library files with the name and path on your system. and you must change the path of snort_dynamicpreprocessorvariable.
C:\Snort\lib\snort_dynamiccpreprocessor
You need to do this to all library files in the “C:\Snort\lib” folder. The old path might be: “/usr/local/lib/…”. you will need to replace that path with your system path. Using C:\Snort\lib
14. Change the path ofthe “dynamicengine” variable value in the “snort.conf” file..

Example:

```
dynamicengine C:\Snort\lib\snort_dynamicengine\sf_engine.dll
```

15 Add the paths for “include classification.config” and “include reference.config” files.

```
include c:\snort\etc\classification.config
include c:\snort\etc\reference.config
```

16. Remove the comment (#) on the line to allow ICMP rules, if it is commented with a #.

```
include $RULE_PATH/icmp.rules
```

17. You can also remove the comment of ICMP-info rules comment, if it is commented.

```
include $RULE_PATH/icmp- info.rules
```

18. To add log files to store alerts generated by snort, search for the “output log” test in snort.conf and add the following line:

```
output alert_fast: snort-alerts.ids
```

19. Comment (add a #) the whitelist $WHITE_LIST_PATH/white_list.rules and the blacklist

Change the nested_ip inner , \ to nested_ip inner #, \

20. Comment out (#) following lines:

```
#preprocessor normalize_ip4
#preprocessor normalize_tcp: ips ecn stream
#preprocessor normalize_icmp4
#preprocessor normalize_ip6
#preprocessor normalize_icmp6
```

21. Save the “snort.conf” file.

22. To start snort in IDS mode, run the following command:

```
snort -c c:\snort\etc\snort.conf - l c:\snort\log - i 3
```

(Note: 3 is used for my interface card)

Ifa log is created, select the appropriate program to open it. You can use WordPard or NotePad++ to read the file.

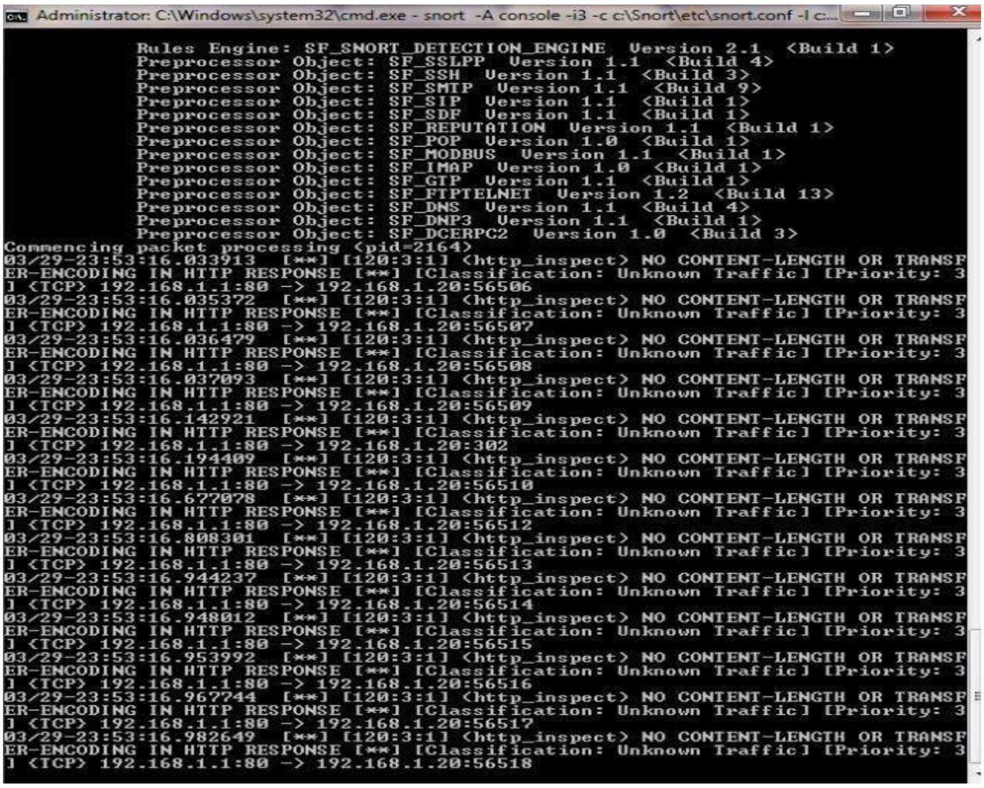
To generate Log files in ASCII mode, you can use following command while running snort in IDS mode:

```
snort -A console - i3 -c c:\Snort\etc\snort.conf -l c:\Snort\log -K ascii
```

23. Scan the computer that is running snort from another computer by using PING or NMap (ZenMap).

After scanning or during the scan you can check the snort-alerts.ids file in the log folder to insure it is logging properly. You will see IP address folders appear.

Snort monitoring traffic –



Administrator: C:\Windows\system32\cmd.exe - snort -A console -i3 -c c:\Snort\etc\snort.conf -l c:...

```
           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 2.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=2164)
03/29-23:53:16.033913  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56506
03/29-23:53:16.035372  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56507
03/29-23:53:16.036479  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56508
03/29-23:53:16.037093  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56509
03/29-23:53:16.142921  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:302
03/29-23:53:16.194409  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56510
03/29-23:53:16.677078  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56512
03/29-23:53:16.808301  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56513
03/29-23:53:16.944237  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56514
03/29-23:53:16.948012  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56515
03/29-23:53:16.953992  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56516
03/29-23:53:16.967744  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56517
03/29-23:53:16.982649  [**] [120:3:1] (http_inspect) NO CONTENT-LENGTH OR TRANSF
ER-ENCODING IN HTTP RESPONSE [**] [Classification: Unknown Traffic] [Priority: 3
] {TCP} 192.168.1.1:80 -> 192.168.1.20:56518
```

RESULT:

Ex.No. : 10 **EXPLORING N-STALKER**

Date :

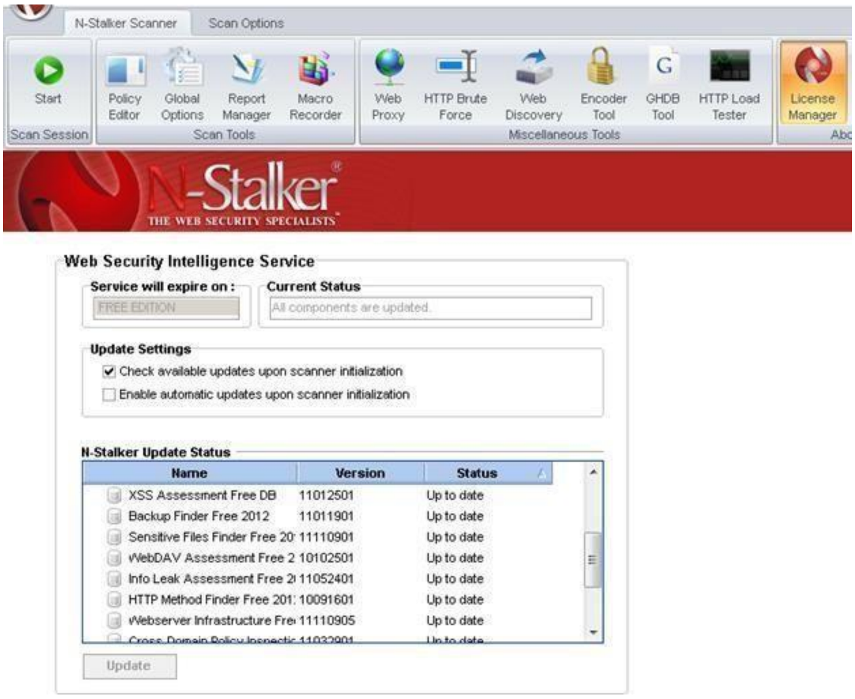
AIM:

To download the N-Stalker Vulnerability Assessment Tool and exploring the features.

EXPLORING N-STALKER:

- N-Stalker Web Application Security Scanner is a Web security assessment tool.
- It incorporates with a well-known N-Stealth HTTP Security Scanner and 35,000 Web attack signature database.
- This toolalso comes in both free and paid version.
- Before scanning the target, go to “License Manager” tab, perform the update.
- Once update, you will note the status as up to date.
- You need to download and install N-Stalker from www.nstalker.com.

1. Start N-Stalker from a Windows computer. The program is installed under Start ➪ Programs ➪ N-Stalker ➪ N-Stalker Free Edition.
2. Enter a host address or a range of addresses to scan.
3. Click Start Scan.
4. After the scan completes, the N-Stalker Report Manager will prompt
5. you to select a format for the resulting report as choose Generate HTML.
6. Review the HTML report for vulnerabilities.



Web Security Intelligence Service

Service will expire on : FREE EDITION

Current Status: All components are updated.

Update Settings

☑ Check available updates upon scanner initialization

□ Enable automatic updates upon scanner initialization

N-Stalker Update Status

Name	Version	Status
XSS Assessment Free DB	11012501	Up to date
Backup Finder Free 2012	11011901	Up to date
Sensitive Files Finder Free 20	11110901	Up to date
WebDAV Assessment Free 2	10102501	Up to date
Info Leak Assessment Free 2	11052401	Up to date
HTTP Method Finder Free 201	10091601	Up to date
Webserver Infrastructure Fre	11110905	Up to date
Cross Domain Policy Inspectic	11032901	Up to date

Update

Now goto “Scan Session”, enter the target URL.

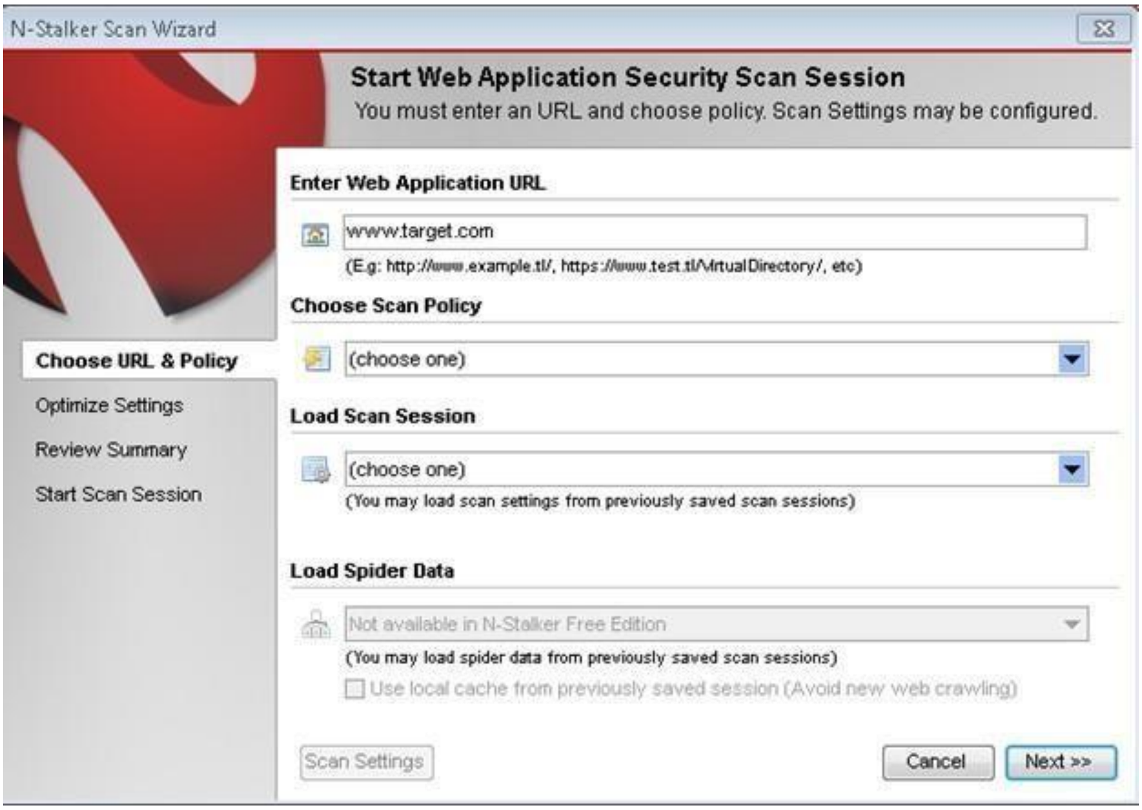
In scan policy, you can select from the four options,

- Manual test which will crawl the website and will be waiting for manual attacks.
- full xss assessment
- owasp policy

- Web server infrastructure analysis.

Once, the option has been selected, next step is “Optimize settings” which will crawl the whole website for further analysis.

In review option, you can get all the information like host information, technologies used, policy name, etc.



N-Stalker Scan Wizard

Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Enter Web Application URL: www.target.com

(E.g: http://www.example.tl/, https://www.test.tl/VirtualDirectory/, etc)

Choose Scan Policy: (choose one)

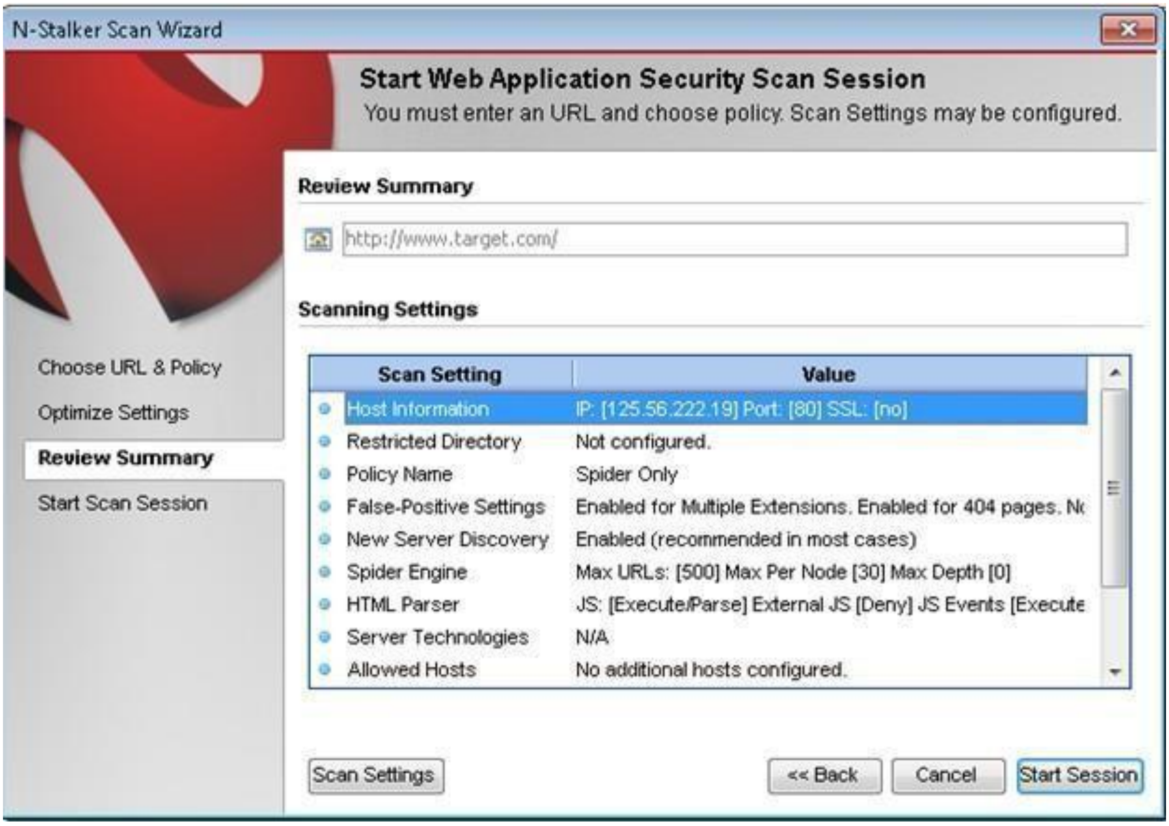
Load Scan Session: (choose one)

(You may load scan settings from previously saved scan sessions)

Load Spider Data: Not available in N-Stalker Free Edition

(You may load spider data from previously saved scan sessions)

□ Use local cache from previously saved session (Avoid new web crawling)



Start Web Application Security Scan Session

You must enter an URL and choose policy. Scan Settings may be configured.

Review Summary

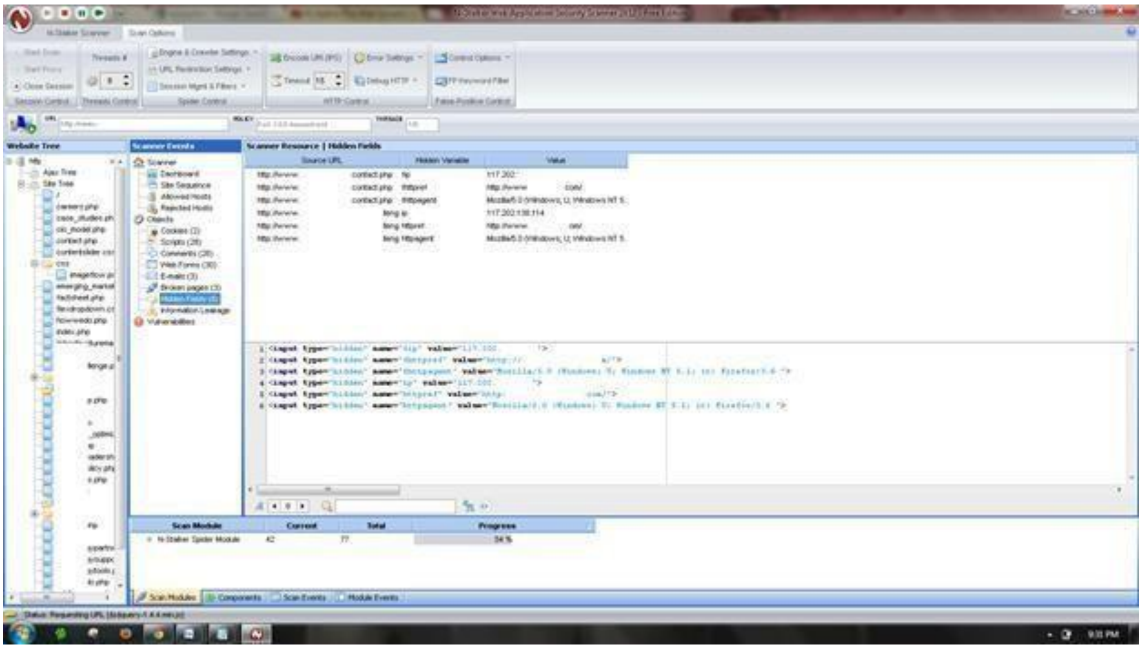
http://www.target.com/

Scanning Settings

Scan Setting	Value
Host Information	IP: [125.56.222.19] Port: [80] SSL: [no]
Restricted Directory	Not configured.
Policy Name	Spider Only
False-Positive Settings	Enabled for Multiple Extensions. Enabled for 404 pages. N
New Server Discovery	Enabled (recommended in most cases)
Spider Engine	Max URLs: [500] Max Per Node [30] Max Depth [0]
HTML Parser	JS: [Execute/Parse] External JS [Deny] JS Events [Execute
Server Technologies	N/A
Allowed Hosts	No additional hosts configured.

Once done, start the session and start the scan.

The scanner will crawl the whole website and will show the scripts, broken pages, hidden fields, information leakage, web forms related information which helps to analyze further.

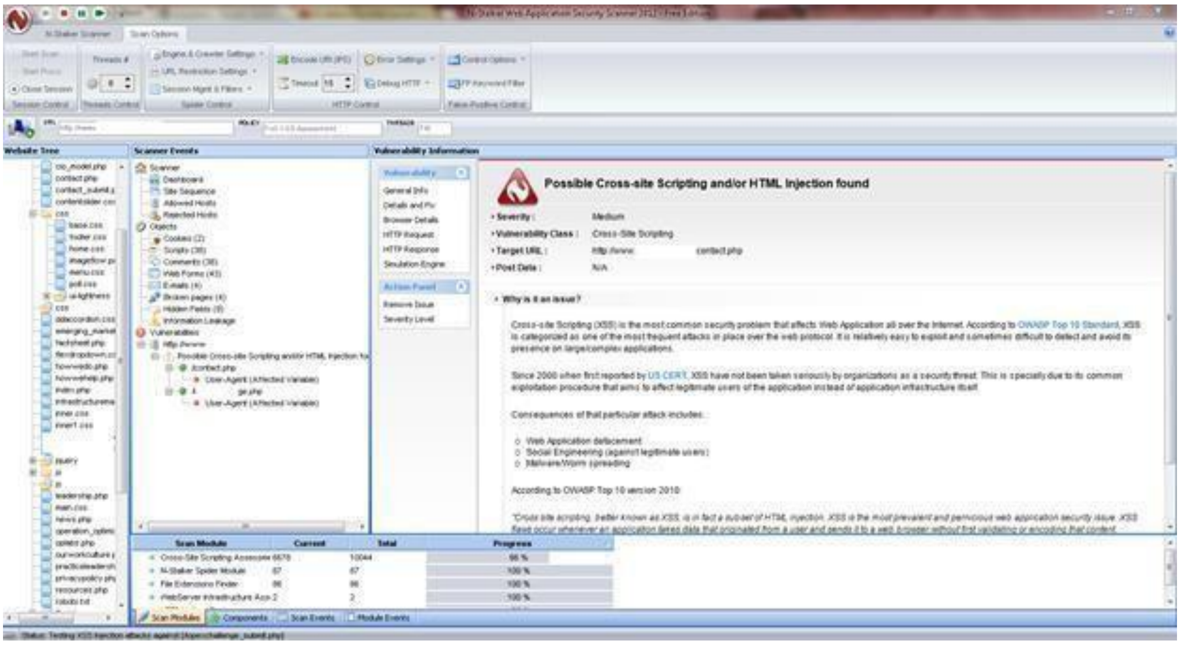


Scanner Resource | Hidden Fields

Source URL	Hidden Variable	Value
http://www contact.php	tip	117.202
http://www contact.php	httpref	http://www com/
http://www contact.php	httpagent	Mozilla/5.0 (Windows; U; Windows NT 5.
http://www	ip	117.202.138.114
http://www	httpref	http://www com/
http://www	httpagent	Mozilla/5.0 (Windows; U; Windows NT 5.

Scan Module	Current	Total	Progress
N-Stalker Spider Module	42	77	54 %

Once the scan is completed, the NStalker scanner will show details like severity level, vulnerability class, why is it an issue, the fix for the issue and the URL which is vulnerable to the particular vulnerability?



Possible Cross-site Scripting and/or HTML Injection found

- Severity : Medium
- Vulnerability Class : Cross-Site Scripting
- Target URL : http://www.   contact.php
- Post Data : N/A

Why is it an issue?

Cross-site Scripting (XSS) is the most common security problem that affects Web Application all over the Internet. According to OWASP Top 10 Standard, XSS is categorized as one of the most frequent attacks in place over the web protocol. It is relatively easy to exploit and sometimes difficult to detect and avoid its presence on large/complex applications.

Since 2000 when first reported by US CERT, XSS have not been taken seriously by organizations as a security threat. This is specially due to its common exploitation procedure that aims to affect legitimate users of the application instead of application infrastructure itself.

Consequences of that particular attack includes:

- Web Application defacement
- Social Engineering (against legitimate users)
- Malware/Worm spreading

According to OWASP Top 10 version 2010

"Cross site scripting, better known as XSS, is in fact a subset of HTML injection. XSS is the most prevalent and pernicious web application security issue. XSS flaws occur whenever an application takes data that originated from a user and sends it to a web browser without first validating or encoding that content.

Scan Module	Current	Total	Progress
Cross-Site Scripting Assessment	6678	10044	66 %
N-Stalker Spider Module	67	67	100 %
File Extensions Finder	86	86	100 %
WebServer Infrastructure Ass	2	2	100 %

Status: Testing XSS Injection attacks against [/open/challenge_submit.php]

RESULT:

Ex.No.: 11a **DEFEATING MALWARE - BUILDING TROJANS**
Date :

AIM:

To build a Trojan and know the harmness of the Trojan malwares in a computer system.

PROCEDURE:

1. Create a simple Trojan by using Windows Batch File (***.bat***)
2. Type these below code in notepad and save it as **Trojan.bat**
3. Double click on ***Trojan.bat*** file.
4. When the Trojan code executes, it will open MS-Paint, Notepad, Command Prompt, Explorer, etc., infinitely.
5. Restart the computer to stop the execution of this Trojan.

TROJAN:

- In computing, a Trojan horse,or Trojan, is any malware which misleads users of its true intent.
- Trojans are generally spread by some form of social engineering, for example where a user is duped into executing an email attachment disguised to appear not suspicious, (e.g., a routine form to be filled in), or by clicking on some fake advertisement on social media or anywhere else.
- Although their payload can be anything, many modern forms act as a backdoor, contacting a controller which can then have unauthorized access to the affected computer.
- Trojans may allow an attacker to access users' personal information such as banking information, passwords, or personal identity.
- ***Example:*** *Ransomware* attacks are often carried out using a *trojan*.

PROGRAM:

OUTPUT:

RESULT:

Ex.No. : 11b **DEFEATING MALWARE - ROOTKIT HUNTER**
Date :

AIM:

To install a rootkit hunter and find the malwares in a computer.

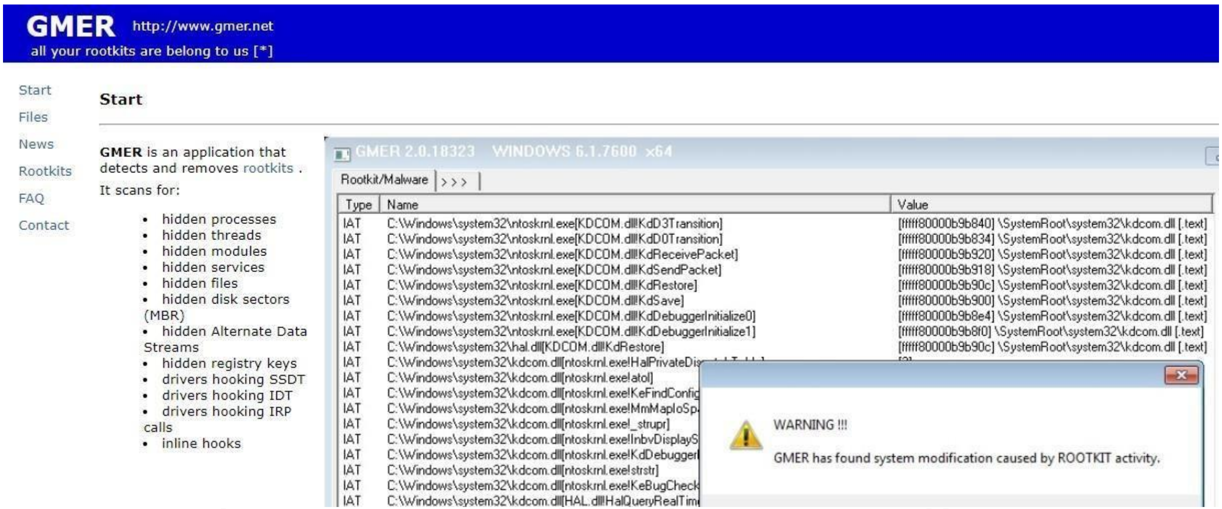
ROOTKIT HUNTER:

- rkhunter (Rootkit Hunter) is a Unix-based tool that scans for rootkits, backdoors and possible local exploits.
- It does this by comparing SHA-1 hashes of important files with known good ones in online databases, searching for default directories (of rootkits), wrong permissions, hidden files, suspicious strings in kernel modules, and special tests for Linux and FreeBSD.
- rkhunter is notable due to its inclusion in popular operating systems (Fedora, Debian, etc.)
- The tool has been written in Bourne shell, to allow for portability. It can run on almost all UNIX-derived systems.

GMER ROOTKIT TOOL:

- GMER is a software tool written by a Polish researcher Przemysław Gmerek, for detecting and removing rootkits.
- It runs on Microsoft Windows and has support for Windows NT, 2000, XP, Vista, 7, 8 and 10. With version 2.0.18327 full support for Windows x64 is added.

Step 1



GMER is an application that detects and removes rootkits .

It scans for:

- hidden processes
- hidden threads
- hidden modules
- hidden services
- hidden files
- hidden disk sectors (MBR)
- hidden Alternate Data Streams
- hidden registry keys
- drivers hooking SSDT
- drivers hooking IDT
- drivers hooking IRP calls
- inline hooks

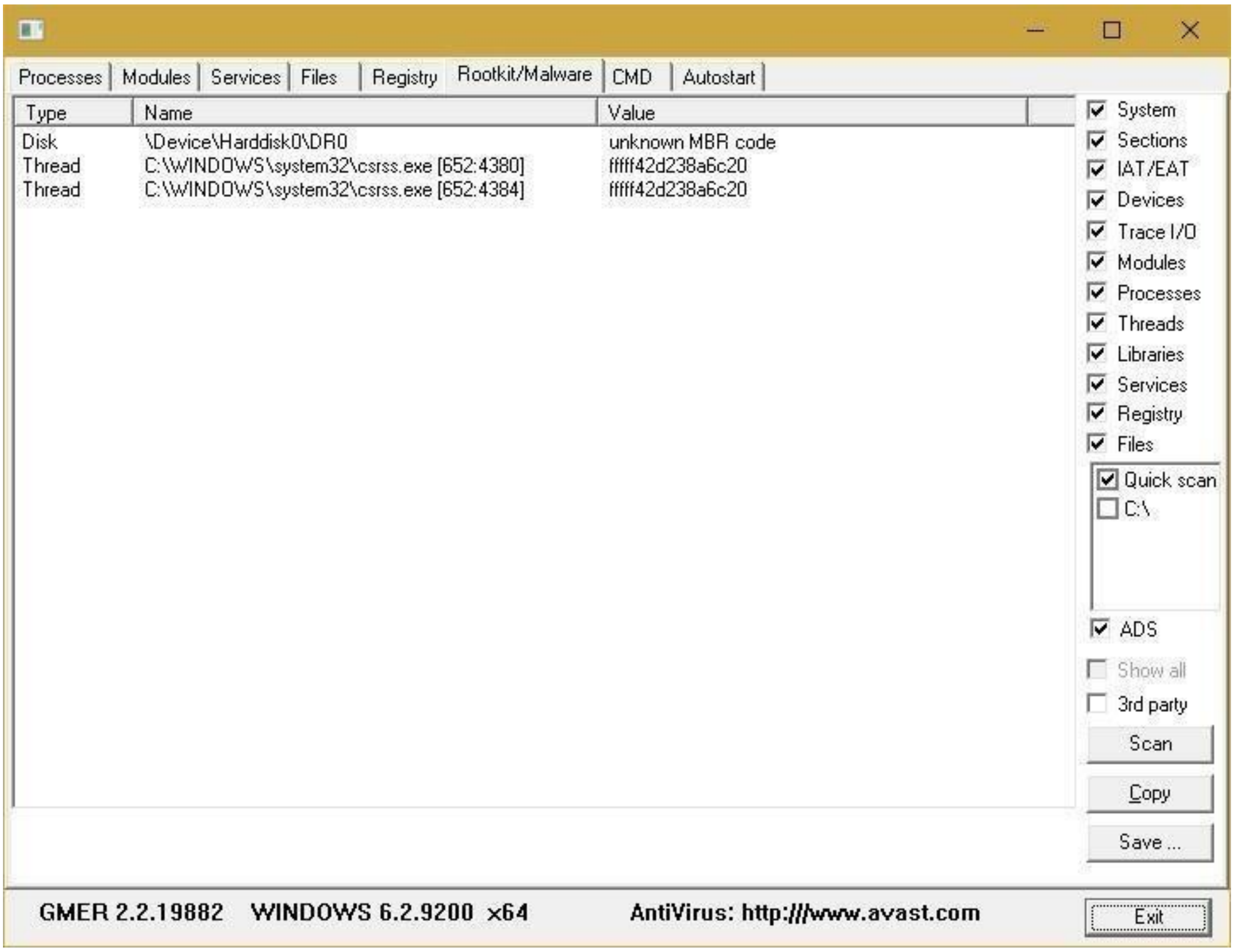
```
Type  Name                                                           Value
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdD3Transition]         [fffff80000b9b840] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdD0Transition]         [fffff80000b9b834] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdReceivePacket]        [fffff80000b9b920] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdSendPacket]           [fffff80000b9b918] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdRestore]              [fffff80000b9b90c] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdSave]                 [fffff80000b9b900] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdDebuggerInitialize0]  [fffff80000b9b8e4] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\ntoskrnl.exe[KDCOM.dll!KdDebuggerInitialize1]  [fffff80000b9b8f0] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\hal.dll[KDCOM.dll!KdRestore]                   [fffff80000b9b90c] \SystemRoot\system32\kdcom.dll [.text]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!HalPrivateDis
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!atol]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KeFindConfig
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!MmMapIoSp
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!_strupr]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!InbvDisplayS
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KdDebugger
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!strstr]
IAT   C:\Windows\system32\kdcom.dll[ntoskrnl.exe!KeBugCheck
IAT   C:\Windows\system32\kdcom.dll[HAL.dll!HalQueryRealTim
```

WARNING !!!

GMER has found system modification caused by ROOTKIT activity.

Visit GMER's website (see Resources) and download the GMER executable.
Click the "Download EXE" button to download the program with a random file name, as some rootkits will close “gmer.exe” before you can open it.

Step 2



Type	Name	Value
Disk	\Device\Harddisk0\DR0	unknown MBR code
Thread	C:\WINDOWS\system32\csrss.exe [652:4380]	fffff42d238a6c20
Thread	C:\WINDOWS\system32\csrss.exe [652:4384]	fffff42d238a6c20

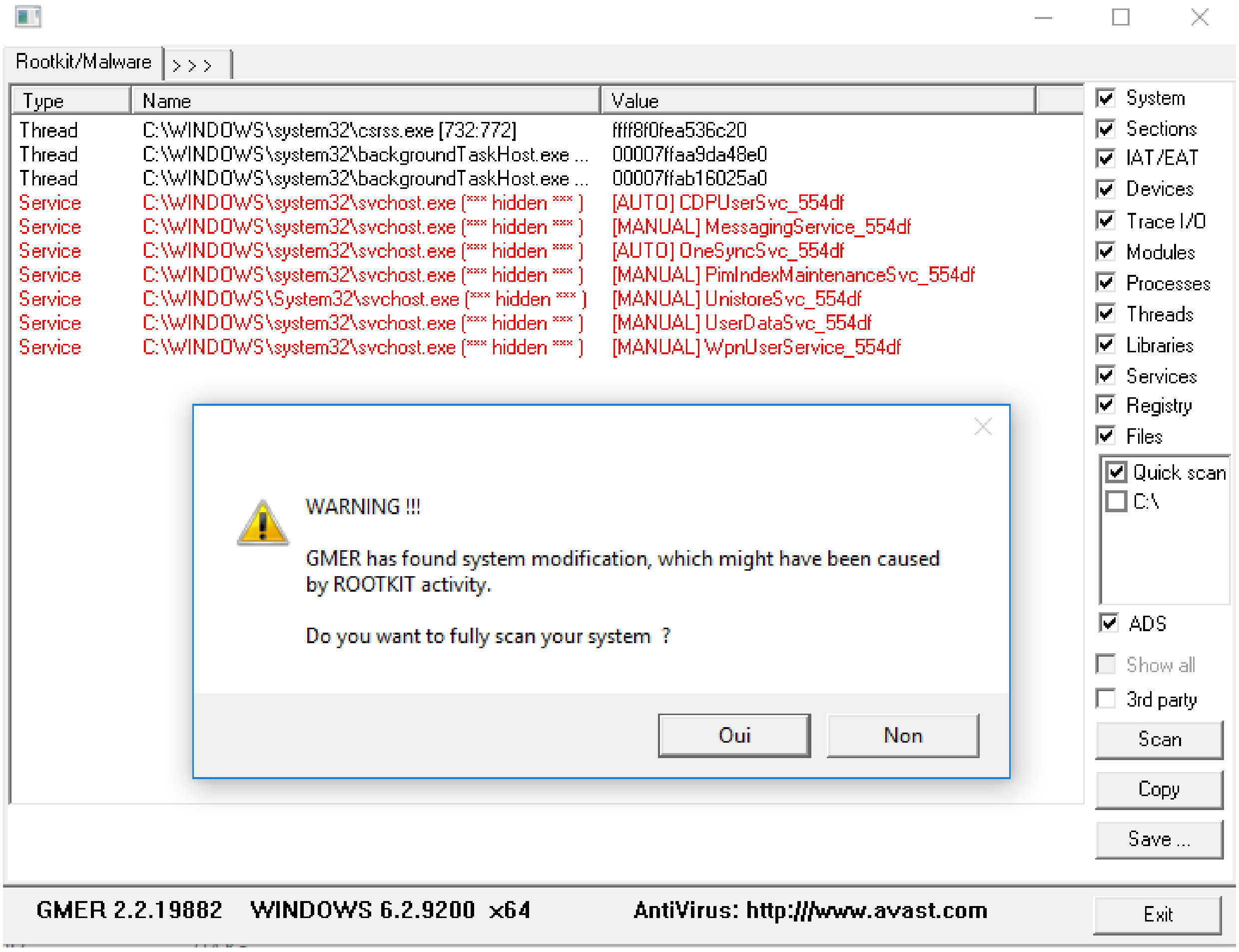
☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Trace I/O
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ Quick scan
□ C:\
☑ ADS
□ Show all
□ 3rd party

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com

Double-click the icon for the program.

Click the "Scan" button in the lower-right corner ofthe dialog box. Allow the program to scan your entire hard drive.

Step 3



Type	Name	Value
Thread	C:\WINDOWS\system32\csrss.exe [732:772]	ffff8f0fea536c20
Thread	C:\WINDOWS\system32\backgroundTaskHost.exe ...	00007ffaa9da48e0
Thread	C:\WINDOWS\system32\backgroundTaskHost.exe ...	00007ffab16025a0
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[AUTO] CDPUserSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] MessagingService_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[AUTO] OneSyncSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] PimIndexMaintenanceSvc_554df
Service	C:\WINDOWS\System32\svchost.exe (*** hidden ***)	[MANUAL] UnistoreSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] UserDataSvc_554df
Service	C:\WINDOWS\system32\svchost.exe (*** hidden ***)	[MANUAL] WpnUserService_554df

☑ System
☑ Sections
☑ IAT/EAT
☑ Devices
☑ Trace I/O
☑ Modules
☑ Processes
☑ Threads
☑ Libraries
☑ Services
☑ Registry
☑ Files
☑ Quick scan
☐ C:\
☑ ADS
☐ Show all
☐ 3rd party

WARNING !!!

GMER has found system modification, which might have been caused by ROOTKIT activity.

Do you want to fully scan your system ?

Oui | Non

GMER 2.2.19882 WINDOWS 6.2.9200 x64 AntiVirus: http://www.avast.com

When the program completes its scan, select any program or file listed in red. Right-click it and select "Delete."

If the red item is a service, it may be protected. Right-click the service and select "Disable." Reboot your computer and run the scan again, this time selecting "Delete" when that service is detected.

When your computer is free of Rootkits, close the program and restart your PC.

RESULT: