Aim: Installation of Operating System on Virtual Machine

Theory:

1. Explain virtualization and types of Virtualization

Virtualization is technology that lets you create useful IT services using resources that are traditionally bound to hardware. It allows you to use a physical machine's full capacity by distributing its capabilities among many users or environments. In computing, virtualization refers to the act of creating a virtual (rather than actual) version of something, including virtual computer hardware platforms, storage devices, and computer network resources.

Types of virtualization:

1. Hardware Virtualization: Hardware virtualization is mainly done for the server platforms, because controlling virtual machines is much easier than controlling a physical server.

2.Server Virtualization: Server virtualization is done because a single physical server can be divided into multiple servers on the demand basis and for balancing the load.

3. Storage Virtualization: Storage virtualization is mainly done for back-up and recovery purposes.

4. Operating System Virtualization: Operating System Virtualization is mainly used for testing the applications on different platforms of OS.

5.Application Virtualization: Application virtualization helps a user to have a remote access of an application from a server

6. Desktop Virtualization: Desktop virtualization allows the users' OS to be remotely stored on a server in the data center

7.Network Virtualization: Network virtualization provides a facility to create and provision virtual networks—logical switches, routers, firewalls, load balancer, Virtual Private Network (VPN), and workload security within days or even in weeks.

2. Explain Hypervisor in detail (Host and Bare Metal Hypervisor)

Hypervisor is a form of virtualization software used in Cloud hosting to divide and allocate the resources on various pieces of hardware. The program which provide partitioning, isolation or abstraction is called virtualization hypervisor. Hypervisor is a hardware virtualization technique that allows multiple guest operating systems (OS) to run on a single host system at the same time. A hypervisor is sometimes also called a virtual machine manager(VMM).

Bare Metal Hypervisor (Type -1 Hypervisor)

Hypervisor runs directly on underlying host system. It is also known as "Native Hypervisor" or "Bare metal hypervisor". It does not require any base server operating system .It has direct access to hardware resources. Examples of Type 1 hypervisors include VMware ESXi, Citrix XenServer and Microsoft Hyper-V hypervisor. Type 1 hypervisors offer much better performance than Type 2 ones because there's no middle layer, making them the logical choice for mission-critical applications and workloads.

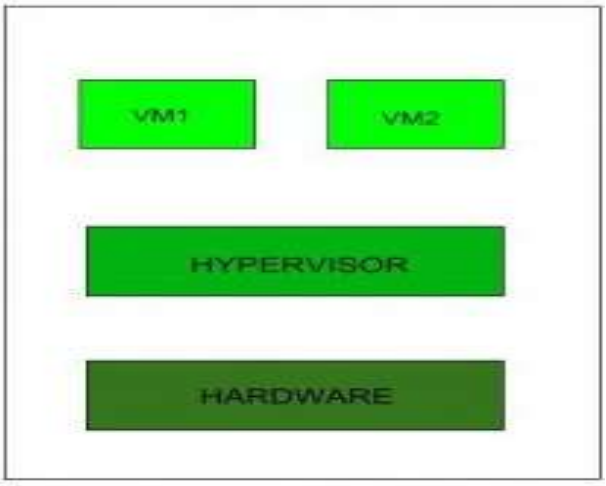


Figure 1 : Bare Metal HyperVisor

Host Hypervisor (Type -2 Hypervisor)

A Host operating system runs on underlying host system. It is also known as "Hosted Hypervisor" .Basically a software installed on an operating system. Hypervisor asks operating system to make hardware calls. Example of Type 2 hypervisor include VMware Player or Parallels Desktop. Hosted hypervisors are often found on endpoints like PCs. They're much simpler to set up, so they're a good bet if, say, you need to deploy a test environment quickly.

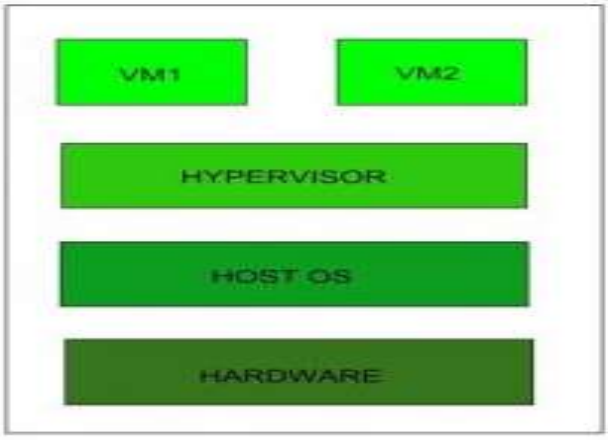


Figure 2 : Host HyperVisor

3. Explain XEN, ESXi and KVM.

XEN
Xen is a type-1 virtual machine, providing services that allow multiple computer operating systems to execute on the same computer hardware concurrently. It was originally developed by the University of Cambridge Computer Laboratory and is now being developed by the Linux Foundation with support from Intel.
A typical environment running Xen consists of different parts. To start with, there's Domain 0. In Xen, this is how you refer to the host operating system (OS), as it's not really a host OS in the sense that other virtual machines (VMs). Domain 0 is only responsible for access to the drivers, and if any coordination has to be done, it will be handled by Domain 0. Apart from Domain 0, there are the other VMs that are referred to as Domain U.

ESXi
VMware ESXi (formerly ESX - Elastic Sky X) is an enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers. As a type-1 hypervisor, ESXi is not a software application that is installed on an operating system (OS); instead, it includes and integrates vital OS components, such as a kernel. The name ESX originated as an abbreviation of. VMware ESXi enables you to:

- Consolidate hardware for higher capacity utilization.
- Increase performance for a competitive edge.
- Streamline IT administration through centralized management.
- Reduce CapEx and OpEx.
- Minimize hardware resources needed to run the hypervisor, meaning greater efficiency.

KVM
Kernel-based Virtual Machine (KVM) is an open source virtualization technology built into Linux. Specifically, KVM lets you turn Linux into a hypervisor that allows a host machine to run multiple, isolated virtual environments called guests or virtual machines (VMs).

KVM is part of Linux. If you've got Linux 2.6.20 or newer, you've got KVM. KVM was first announced in 2006 and merged into the mainline Linux kernel version a year later. Because KVM is part of existing Linux code, it immediately benefits from every new Linux feature, fix, and advancement without additional engineering.

4. What is a Virtual Box?

VirtualBox is open-source software for virtualizing the x86 computing architecture. It acts as a hypervisor, creating a VM (virtual machine) where the user can run another OS (operating system).

The operating system where VirtualBox runs is called the "host" OS. The operating system running in the VM is called the "guest" OS. VirtualBox supports Windows, Linux, or macOS as its host OS.

When configuring a virtual machine, the user can specify how many CPU cores, and how much RAM and disk space should be devoted to the VM. When the VM is running, it can be "paused." System execution is frozen at that moment in time, and the user can resume using it later.

5. Role of Virtualization in cloud computing

Virtualization is the backbone of Cloud Computing; Cloud Computing brings efficient benefits as well as makes it more convenient with the help of Virtualization, not only this, it also provides solutions for great challenges in the field of data security and privacy protection.
In a file or a web server, the usage of purchase, maintenance, depreciation, energy and floor space is double, but by creating virtual web or file server all of our objectives are fulfilled like the use of hardware resources to its maximum, flexibility, improvement in security, reduced cost. Efficient use of resources, increased security, portability, problem free testing, easier manageability, increased flexibility, fault isolation, rapid deployment are the benefits of virtualization.

Virtualization in Cloud Computing:

- For combining local and network resources data storage virtualization.
- For grouping physical storage devices into the single unit
- For reaching the high level of availability or improving availability using virtualization
- Improving performance using virtualization
- Using virtualization using stripping and caching
- Capacity improvement
- A central computer hosting an application to multiple users, preventing the need for installing software repeatedly on every system is virtualization in Cloud Computing. The data from different hard drives, USB drives, and databases are merged into one location increasing its accessibility and security.

The creation of virtual hardware, software, or an operating system or a storage or network device is virtualization in cloud computing. In IT virtual changes occur more rapidly than in a physical environment. The changes occurring has to be managed, such changes are scalable and agile because of virtualization in Cloud Computing.

6. Advantage and limitation of virtualization

Advantages:

1. Performance : Gain better performance and efficiency from resources in the existing computing components, using CPU virtualization.

2. Distribution Security : Virtualization boost virtual machine (VM) security. Since VMs are logically separated from each other, a malware attack or other software glitch on one VM won't affect other VMs.

3. Cost : Save money on hardware. Virtualization software involve less cost, and also require lesser hardware to run than physical machines.

4. Management : Gain peace of mind. VMs provide better reliability in terms of disaster recovery as well as better backup and retrieval capabilities.

5. Uptime : Virtualization has the capability to prevent unnecessary downtime by making use of resources the maximum. Even budget friendly virtualization services can offer an uptime of almost 99.9% today. This can be especially beneficial for small businesses which uses data for testing.

Limitations:

1. Implementation : Virtualization is highly cost effective still it needs more investment when it comes to implementation. This is because at some instance the H/w and S/w are required which means that devices needs to be purchased to make the virtualization possible. This can mainly effect the providers of virtual environment. However it is one time investment which long term benefits.

2. Security : Data security is often questioned in a virtualized environment since the server is managed by managed by the third party providers. Therefore, it is important to choose the virtualization solution wisely so that it can provide adequate protection.

3. Availability : The issue with the availability can come from the virtualization servers. The virtualization servers has the tendency to go offline. Hence, the websites which are hosted will also be failed. This is solely controlled by the third party providers, there is nothing the user can do about it.

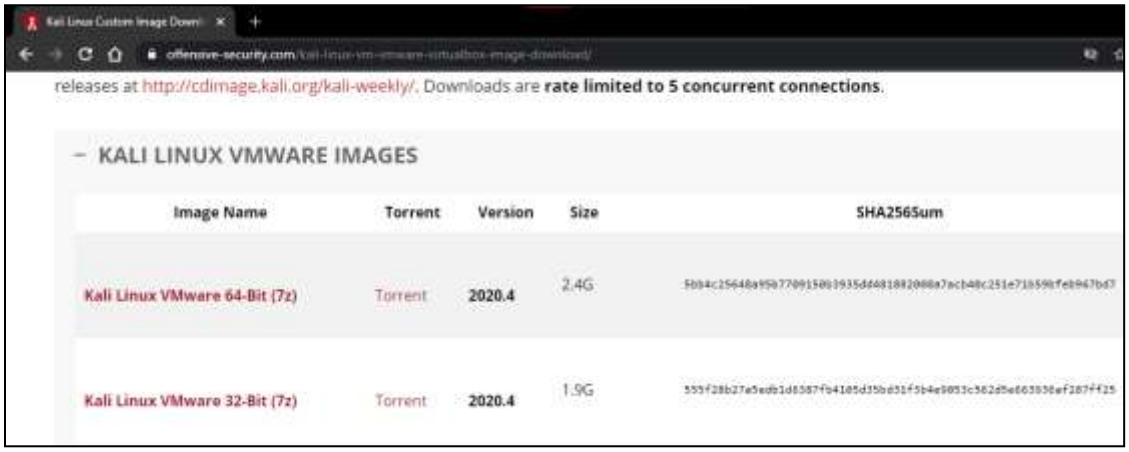
4. Scalability : There is an upper bound of number of machines we can have in a data center. Every machine will have it OS and it will run the applications. When we are out of space, we cannot scale for our running applications.

5. It requires several links in a chain that must work together cohesively : For example of saving a document file. With a local storage device, like a flash drive or HDD, you can save the file immediately and even create a backup. Using virtualization, your ISP connection would need to be valid. Your LAN or Wi-Fi would need to be working. Your online storage option would need to be available. If any of those are not working, then you’re not saving that file.

Installation of Operating System on Virtual Machine:

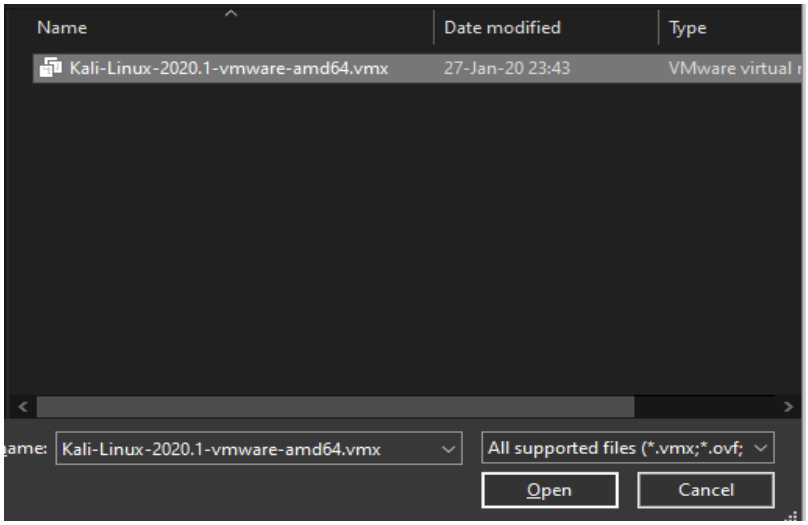
1. Explain steps to install OS on VM using KVM/Virtual Box with screenshots.

Step 1 : Downloading Kali Linux image from Offensive security

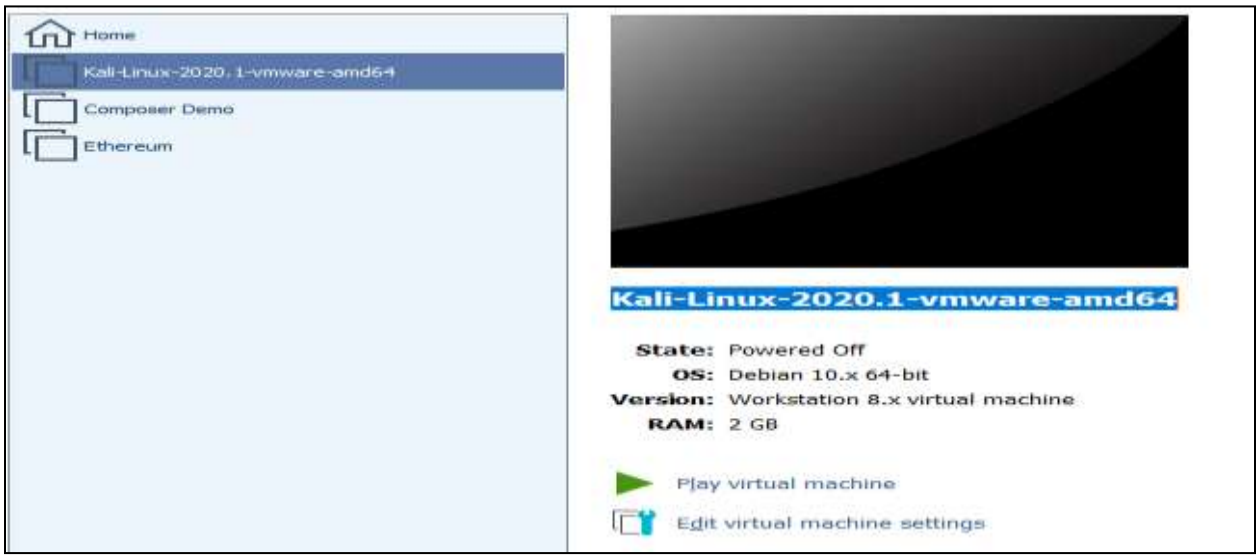


Step 2 : Go to File

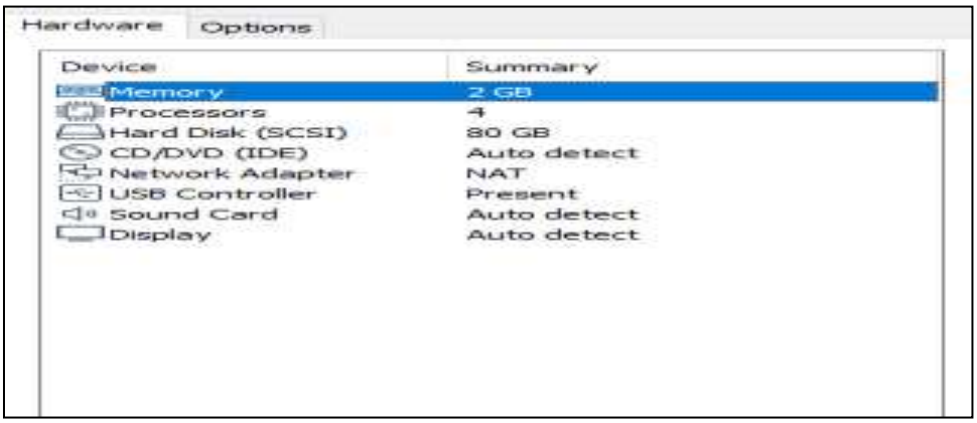
Step 3 : Click on New Virtual Machine for creating a machine OR click on Open.. to directly install a .vmdk/.ovf/.ova/.vmx (We will use Open.. to Install Kali Linux OS using .vmx)



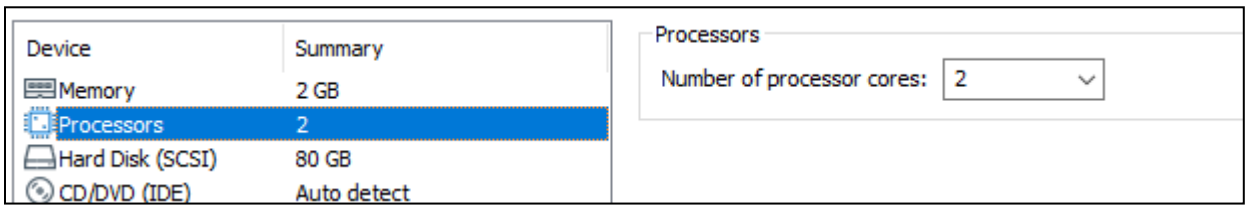
Step 4 : Now VMware will configure this .vmx file



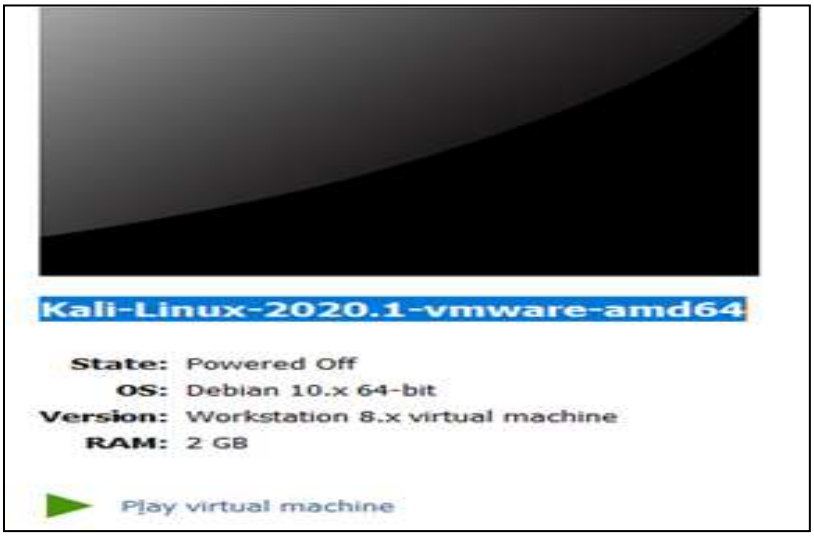
Step 5: Click on Edit Virtual machine settings



Here one can setup all the required settings for the Os to run properly like RAM, ROM, number of processors etc. We will change the processor count to 2 instead of 4. After that click "OK"



Step 6: Now we click on "play virtual machine"



Step 7: Now we are fully setup for using Kali Linux by using its default username and password we can login.

CONCLUSION:

- From this experiment, we learnt about creating virtual machines, hypervisors and information about virtualization.
- There are multiple criteria to decide which hypervisor suits a company, factors like Flexibility, Scalability, Usability, Availability, Reliability, Efficiency, Reliable support are important to decide which hypervisor to select.
- For example for personal use and smaller deployments, you can go for one of the type 2 hypervisors. If we want high performance we should opt for Bare metal or Type 1 hypervisor because there is no middle layer, making them the logical choice for mission-critical applications and workloads.
- To resolve limitations of virtualization, we use containers by getting rid of kernel copies in VM. We can run containers without kernels which will be provided by the HostOS.
- Containers are a package that will contain everything , which solves the problem of software dependencies and installation and helps to run VM with same OS on one kernel. For security limitations, it uses namespaces and cgroups(Control Groups) which creates isolation and abstraction so one user cannot access data from the other.
- Finally, we installed Kali Linux operating system in VMware

REFERENCES:

1. https://www.redhat.com/en/topics/virtualization/what-is-virtualization
2. https://www.geeksforgeeks.org/virtualization-cloud-computing-types/
3. https://www.geeksforgeeks.org/hypervisor/
4. https://www.vmware.com/topics/glossary/content/hypervisor
5. https://xenproject.org/
6. https://www.vmware.com/in/products/esxi-and-esx.html
7. https://www.redhat.com/en/topics/virtualization/what-is-KVM#:~:text=Kernel%2Dbased%20Virtual%20Machine%20(KVM,or%20virtual%20machines%20(VMs).
8. http://offensive-security.com/kali-linux-vm-vmware-virtualbox-image-download/