1. [1.5x2=3 points] What is the benefit of using a virtual machine in the following scenarios:

(a) An operating system developer for MegaSoft, who is testing out a new kernel feature for the Doors operating system.

Ans. A few benefits of using virtual machines for OS development are:-

- **Isolation: Since virtual machines offer a high level of isolation, programmers can test out various operating system configurations without having an impact on their host systems. This isolation ensures a stable development environment by preventing potential conflicts and system breakdowns.**

- **Parallel Development: By allowing many instances of an operating system to run concurrently on the same physical computer, virtual machines enable parallel development. When working on multiple operating system components or features at once, this functionality is useful, increasing overall development efficiency.**

- **Compatibility Testing: The platform provided by virtual machines is ideal for compatibility testing. To test the operating system on diverse hardware and software combinations, developers can build virtual machines with alternative configurations. This assists in locating and resolving compatibility problems early in the development process.**

- **Resource Management: Developers can allocate particular resources, such as CPU cores, memory, and storage, to each instance using virtual machines. This feature gives developers fine-grained control over resource usage, enabling them to emulate various hardware setups and enhance performance for particular settings.**

(b) An employee of Bolton Anti-virus, who has received a new malware sample, and needs to figure out what the malware does.

Ans. A few benefits of using virtual machines for threat detection are:-

- **Reproducibility: Threat detection investigations can be replicated since virtual computers can be simply copied or returned to a known clean condition. This is very helpful for evaluating malware samples, testing various security technologies, or replicating particular attack scenarios. Each test begins with a consistent baseline because there is the option to go back to a clean state.**

- **Safe Environment: A controlled and secure environment is provided by virtual computers for the examination of possibly harmful software or suspicious data. Without jeopardising the stability of the host system, security researchers and analysts can run questionable code or potentially malicious applications within a virtual machine. If the software or code behaves maliciously, it may be quickly isolated and eliminated.**

- **Network Segmentation: Network segmentation is possible thanks to the configuration of virtual machines with distinct network interfaces or virtual networks. With the help of this capability, network activity within the virtual machine may be tracked and analysed without affecting the host network. It assists in identifying any unusual patterns or behaviours and in capturing and inspecting possibly harmful network activity.**

- **Collaboration and Sharing: Security researchers and analysts can readily exchange virtual machine images, encouraging cooperation and knowledge exchange. Researchers can duplicate their threat detection environment by distributing pre-configured virtual PCs with appropriate security tools and configurations. This fosters exchange of threat intelligence, collaboration, and research acceleration.**

2. [1.5x2=3 points] ChatTPG is an AI-based company that lets customers get answers from an AI chatbot. It runs its service from a large data center containing many servers. To serve customers using its software, ChatTPG is considering two options:

(a) Install the ChatTPG software on each of the servers. Customers will log into the servers directly and interact with the chatbot.

(b) Run hypervisors on the servers, with multiple virtual machines running on each hypervisor. The virtual machines will be equipped with the ChatTPG software. Customers will log into the virtual machines and interact with the chatbot there.

Which option would be better? Why? Please explain your choice with detailed justifications.

Ans. Running hypervisors on the servers, with multiple VMs would be the ideal choice for the ChatTPG service. The reasons are as follows:-

- **Efficient Resource Utilization: ChatTPG can use virtual machines to make the most of their server resources. Each hypervisor supports numerous virtual machines, thus multiple clients can effectively share the server's total capacity. As a result, it is possible to more effectively allocate resources and scale up or down in response to changes in consumer demand. In order to adapt to changing needs, it offers flexibility in terms of scaling up or down the number of Vms.**

- **Isolation and Security: Compared to installing ChatTPG software directly on each server, running it within distinct VMs gives superior isolation and security. The danger that one customer's actions will have an influence on the other customers or the underlying host system is minimised because each VM functions separately in its own isolated environment. One VM's security flaws or vulnerabilities are limited to that particular instance, lowering the entire attack surface.**

- **Easy Management and Maintenance: The management and upkeep of the ChatTPG software is simplified with VMs. The VM templates allow for updates, patches, and configuration changes, ensuring consistent and effective management across numerous instances. If a problem emerges in one VM, it can be fixed separately from the rest of the system or other VMs. Additionally, taking snapshots and going back to earlier states makes troubleshooting easier and decreases downtime.**

- **Scalability and Flexibility: Compared to deploying applications on servers directly, virtual machines offer more flexibility and scalability. By adding or deleting VMs as necessary, ChatTPG may quickly scale up or down their capacity with virtual machines. This flexibility enables effective resource allocation, particularly during peak periods or when load balancing across numerous servers is required. Additionally, it enables ChatTPG to provide several software configurations or versions on various VMs in order to meet the varied needs of their clients.**

- **Easy Deployment and Testing: For ChatTPG, using VMs makes deployment easier. It is possible to construct VM templates with the required software and configurations, speeding up the provisioning of new instances. Additionally, the ability to clone virtual machines (VMs) or create templates makes it simple to replicate and test various software versions or experimental features without affecting the production environment.**