Homework: Week 15

Tanu Shree

(Q1)

The guest OS's current state is entirely contained and can be saved to a file without risk.
Later, the state can be restored by loading it from the file. The virtual machine can be replicated by distributing the file that contains the state. The virtual machine can be moved in a similar way by being saved to a file and then restored on another host. This enables consolidation of multiple virtual machines on a single host. One de facto creates a checkpoint by saving the state of a virtual machine to a reliable storage system. One can return to the most recent saved state if the system crashes.

The native OS's state includes not only the memory state but also the state of all the
All registers must be in their current state in order to be stored on disks without being altered before the process is complete.

As a result, while it is possible to store the state of a virtual machine on reliable storage, doing the same for a native OS is practically impossible.

(Q2)

The hypervisor needs to be able to discover the guest OS's page tables without any API to do this. The method involves intercepting the sensitive instruction in which the guest OS loads a page table into CR3, executing a function called "handle CR3" instead, and using that information to construct a shadow page table that can be used to translate virtual addresses to addresses in the main memory of the machine.

If the guest OS later executes a process-level context switch, it has to load the page table of the new process into CR3. This again invokes the handle CR3 function of the hypervisor, which loads the shadow page table of the new process and the funcion returns.

When a page fault occurs, the page fault handler of the hypervisor takes over and checks the page table to see if the page table entry there is valid. If it is not, this means that the page fault is genuine and the hypervisor directs it to the guest operating system for handling. The guest OS then handles the page fault and the page fault handler returns.