MVE – Assignment

Unit 4

Vishal r

RA2012033010001

1)Virtual Machine Security architecture, security parameters

VMware Infrastructure incorporates a number of features that directly address the security concerns of the most demanding datacenter environments. Some of these include

• A virtualization layer designed from the ground up to run virtual machines in a secure manner while still providing high performance

• Compatibility with SAN security practices. VMware Infrastructure enforces security policies with LUN zoning and LUN masking.

• Implementation of secure networking features. VLAN tagging enhances network security by tagging and filtering network traffic on VLANs, and Layer 2 network security policies enforce security for virtual machines at the Ethernet layer in a way that is not available with physical servers.

• Integration with Microsoft® Active Directory. VMware Infrastructure allows you to base access controls on existing Microsoft Active Directory authentication mechanisms. VMware Infrastructure 3, the latest generation of VMware datacenter products, includes several key enhancements that further address the security needs and challenges of modern IT organizations:

• Custom roles and permissions. VMware Infrastructure enhances security and flexibility with user-defined roles. You can restrict access to the entire inventory of virtual machines, resource pools and servers by assigning users to these custom roles.

• Resource pool access control and delegation. VMware Infrastructure secures resource allocation at different levels in the company. For example, when a top-level administrator makes a resource pool available to a department-level user, all virtual machine creation and management can be performed by the department administrator within the boundaries assigned to the resource pool.

• Audit trails. VMware Infrastructure maintains a record of significant configuration changes and the administrator who initiated each one. You can export reports for event tracking.

• Session management. VMware Infrastructure enables you to discover and, if necessary, terminate Virtual Center user sessions.

VMware Infrastructure Architecture and Security Features From a security perspective, VMware Infrastructure consists of several major components:

• The virtualization layer, consisting of the VM kernel and the virtual machine monitor

• The virtual machines

• The ESX Server service console

• The ESX Server virtual networking layer

• Virtual storage

• Virtual Center

CPU Virtualization Binary translation is a powerful technique that can provide CPU virtualization with high performance.

The VMM uses a translator with the following properties:

• Binary — Input is binary x86 code, not source code.

• Dynamic — Translation happens at run time, interleaved with execution of the generated code.

• On demand — Code is translated only when it is about to execute. This eliminates need to differentiate code and data.

• System level — The translator makes no assumptions about the code running in the virtual machine. Rules are set by the x86 architecture, not by a higher-level application binary interface.

• Sub setting — The translator’s input is the full x86 instruction set, including all privileged instructions; output is a safe subset (mostly user-mode instructions).

• Adaptive — Translated code is adjusted in response to virtual machine behavior changes to improve overall efficiency.