# Assignment#2

**Swapnil Hasabe** **sdh140430**

**Question 1: Describe advantages and disadvantages of hypervisor monitoring the guest Operating System**.

**Advantages:**

1. Strong Isolation: The hypervisor thus provides strong isolation between the security monitors and the attacks present in the guest OS. They could also largely defend against false data generation attacks.
2. Hypervisor allows authentication to guest operating systems which ensures security and also provides access control on who can read and write the data.
3. Transparent Deployment: To deploy a security monitor at the hypervisor layer, there is no need for an account in the guest OS, also no need to install the software inside the OS. Instead, everything can happen transparently at the hypervisor layer without even disrupting services.
4. Complete View: Hypervisor has full access to all of the memory, register, and disk state of the VM on which the OS run. Application's state, as well as the kernel state, including those invisible ones hidden by attackers can be viewed.
5. The hypervisor also reduces denial of service conditions in the guest operating systems. It manages the excess resource used by other OS
6. When a Virtual Machine crashes, the hypervisor takes care of guest operating system.
7. The hardware used for running multiple operating systems. This increases the efficient use of processor and memory resources and also reduces the cost and complexity as the storage setup is simplified.
8. When the hypervisor stores data, it encapsulates all the components and applications of the guest operating systems into an entity called image. The images when stored like files on the hard drives can be easily transferred to other systems. This helps to move data between systems easily.

**Disadvantages:**

1. Slow Speed: Hypervisor has to perform additional address translation (what it observes is physical memory addresses, and it has to translate between those and the guest's virtual addresses) and world switching that traps to the hypervisor for security checks and monitoring. It becomes slow.
2. Security of Hypervisor can be weakening by rebooting and changing all settings of access control management. Authorization by using password can be broken by attacker.
3. If guest operating systems keeps data after leaving hypervisor, that can be lead to the attack.
4. When considering the cost and maintenance, hypervisor just adds up to be an additional layer of technology that has to be managed.
5. The sharing of information through clipboards between one guest operating system and hypervisor can be a chance for attacker as the data on clipboards is also accessible by other guest operating systems. There is always need of secured channel which very difficult to maintain.
6. The hypervisor has the disadvantage of being potentially attacked in one of two ways, from either the network layer or from the host running on that hypervisor

**Question 2: Provide a short survey of the various attacks to the hypervisor**

A hypervisor attack is an exploit in which an intruder takes advantage of vulnerabilities in the program used to allow multiple operating systems to share a single hardware processor.

1. At the Black Hat USA 2015 and DEF CON 23 conferences, a group of Intel Security researchers from the Advanced Threat Research team demonstrated that some hypervisors are vulnerable to attacks through system firmware launched from administrative guests. These attacks led to successful installation of a rootkit in the system firmware (such as BIOS), privilege escalation to the hypervisor privileges, and exposure of hypervisor memory contents

2. Hypervisors employ a range of techniques to isolate software and I/O devices, block escapes from any compromised virtual machine to any other virtual machine, and protect each virtual machine's secrets from the others, including their operating systems. However, these protections fall short when the physical machine system firmware is infected with a rootkit or when a compromised virtual machine is able to exploit vulnerabilities in the firmware.

3. In this case, the firmware rootkit was installed by re flashing the system firmware while it wasn't adequately protected in non-volatile flash memory. Physical access controls should prevent this in some cases

4. A rootkit can open a backdoor for an attacker to access the memory contents of all other virtual machines by adding entries to the hardware-assisted page tables and mapping all of DRAM to the attacker's guest address space.

5. Hypervisor involves in TCP/IP connection establishment, this result in the hypervisor being locatable on the network and consequently susceptible to traditional network enumeration attacks such as Nmap (nmap.org, 2012) and Nessus (Tenable, 2012)

6. Hypervisor can be attacked from the guest or virtual machine that is much more dangerous and an unfamiliar concept, especially for companies invested in the cloud computing or hosting servers in large datacenters.

7. Real world Attack of Hypervisor: CloudBurst Attack on VMware Workstation which exploited vuln in VMware Display functions. It allows code to be executed in host from within guest VM.

8. Breaking hypervisor isolation and attacking — or exploiting — neighboring virtual machines is a prominent goal of cyber criminals.

9. An attacker can exploit other vulnerabilities if the hypervisor allows direct access to the firmware interfaces. For example, we comprised the hypervisor using the resume boot script table in memory that runs when a machine resumes from a sleep state (S3). From a privileged guest, this critical script table structure was changed to access the hypervisor memory spaces.

Question 3:

Three cloud Frameworks and compare their security features

| Amazon AWS | Google | Microsoft Azure |
|---|---|---|
| Amazon EC2 provides Host operating System, guest operating system and complete firewall solution. | The JVM runs in a secured "sandbox" environment to isolate application for service and security.<br>Python interpreter also runs in secured "sandbox" environment to isolate service and security | Filtering routers is the famous feature of azure. |
| It contains shared cloud network | No shared cloud network | No shared cloud network |
| Contains Virtual Private Cloud Network | Contains Virtual Private Cloud Network | Contains Virtual Private Cloud Network |
| Firewalls: Security groups | Firewalls rules using tags | Firewall endpoints only |
| Secure extension using IPSec | In Beta | Secure extension using IPSec |
| Remote Access to Individual Cloud Servers: SSH/RDP | Remote Access to Individual Cloud Servers: SSH/RDP | Remote Access to Individual Cloud Servers: SSH/RDP |
| No Identity Based Access Management | No Identity Based Access Management | No Identity Based Access Management |
| No User Based VPN Access | No User Based VPN Access | User Based VPN Access |
| Amazon S3 is accessible via SSL encrypted endpoints | GO compiler runs inside a secured "sandbox " environment | Cryptographic Protection of Message |
| Simple DB API provides domain level controls that only permit authenticated access by domain creator. | | Software Security patch Management |
| Simple DB access can be granted based on AWS Account ID. | | Centralized monitoring correlation |
| | | Network Segmentation |
| | | Service Administration Access |
| | | Azure compute provides optional sandboxing technology to limit harm to infrastructure |
| | | Provide VM to customers, giving access to security options available in windows server. |