Assignment #2

1. **Describe advantages and disadvantages of hypervisor monitoring the guest operating systems**

A. Advantages:

- Although the two types of security monitors can perform most of the same functions (e.g., identifying malware, detecting intrusions), moving monitoring functionality out-of-VM has tremendous benefits. We can have:
- **Strong isolation** (tamper resilience): There is a switch for control passes between the hypervisor and guest OS. Thus, the hypervisor provides strong isolation between the attacks present in guest and security monitors. If there are any vulnerabilities present in hypervisor, then it makes M and P tamper resilient, as it is located below guest OS. If the virtual machine directly extracts raw data, then there is a large possibility to defend against false data generation attacks, from attackers who generate false data.
- **Transparent deployment**: There is no need for an account in the guest OS or do we need to have any need to install software inside OS to deploy a security monitor at hypervisor layer. Instead, without even disrupting services, everything can happen transparently at the hypervisor layer. (e.g. many read-only introspection techniques can be transparently deployed during runtime).
- **Complete view**: Another advantage is that the hypervisor has full access to all the memory, register, and disk state of the VM on which the OS runs. Each application's state, as well as the kernel state, including those invisible ones hidden by attackers, can be observed which is often challenging to achieve.
- **High cost savings**: VM also provides system developers unrestricted accesses to virtualized resources. They can also save a snapshot of the state of the guest OS, which can be analyzed later without affecting the performance of the running VM.
- **Less vulnerability**: VM often only needs to trust the underlying hypervisor, which has a smaller code base. For example, the Xen hypervisor has less than one twelfth the number of lines of code than the Linux kernel; this smaller attack surface leads to fewer vulnerabilities.

Disadvantages:

- Although hypervisor monitoring the guest operating systems, it also has limitations.
- **No abstractions**: There are no guest OS abstractions. Therefore, all VM solutions face a challenge that must be addressed to perform effective monitoring; they must bridge the semantic gap caused by moving monitors outside of the guest OS.
- **Slow speed**: In addition, hypervisor monitoring must perform additional address translation and world switching that traps to the hypervisor for security checks and monitoring. It therefore usually is slower, although recently there were efforts to improve performance of the world switching.

2. Provide a short survey of the various attacks to the hypervisor

A.

- The hypervisor or virtual machine monitor is an additional layer of software between an operating system and hardware platform that is used to operate multi-tenant virtual machines and is common to IaaS clouds. Besides virtualized resources, the hypervisor normally supports other application programming interfaces to conduct administrative operations, such as launching, migrating, and terminating virtual machine instances.
- Compared with a traditional, non-virtualized implementation, the addition of a hypervisor causes an increase in the attack surface. That is, there are additional methods (e.g., application programming interfaces), channels (e.g., sockets), and data items (e.g., input strings) an attacker can use to cause damage to the system
- Several examples illustrate the types of attack vectors possible. The first is **mapping the cloud infrastructure**. Although it seems as a difficult task to perform, researchers have demonstrated an approach with a popular IaaS cloud.

a. By using network probes, assigned IP addresses and domain names were analyzed to identify service location patterns and launching multiple virtual machine instances from multiple cloud consumer accounts.
b. Building on that information and general technique, the location of target virtual machine could be identified, and new virtual machines instantiated to be eventually co-resident with the target.

- Once a suitable target location is found, the next step for the guest virtual machine is to bypass or **overcome containment by the hypervisor** or to takedown the hypervisor and system entirely.

a. Weaknesses in the processing of instructions and provided programming are common targets for uncovering vulnerabilities to exploit.
b. For example, a serious flaw that allowed an attacker to write to an arbitrary out-of-bounds memory location was discovered in the power management code of a hypervisor by fuzzing emulated I/O port
c. A denial of service vulnerability, was also uncovered in a virtual device driver of a popular virtualization software product

- **Attack Vectors**. Multi-tenancy in virtual machine-based cloud infrastructures, together with the subtleties in the way physical resources are shared between guest virtual machines, can give rise to new sources of threat.

a. The malicious code can escape the confines of its virtual machine and interfere with the hypervisor or other guest virtual machines is a serious threat.
b. Transitioning a virtual machine between hypervisors on different host computers without halting the guest OS, and this ability is called Live migration. Other features provided by virtual machine monitor environments to facilitate systems management, also increase software size and complexity and potentially add other areas to target in an attack.

3. Select three cloud computing frameworks (e.g., Amazon, IBM, Microsoft clouds) and compare their security features

A.

AWS	IBM	Microsoft
Certificate Manager -Lets you easily provision, manage, and deploy Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates. -removes the time-consuming manual process of purchasing, uploading, and renewing SSL/TLS certificates.	**Certificate Manager** - Security certificate repository - Integration with IBM cloud services - Protect and secure apps with SSL/TLS - Avoids outages	**Certificate Manager** - Service certificates are attached to cloud services and enable secure communication - X.509 v3 Certificates used in Azure and can be signed by another trusted certificate or self-signed. -A self-signed certificate is signed by its own creator.
Identity and Access Management -enables you to securely control access to AWS services and resources for your users. Using IAM, you can create and manage AWS users and groups, and use permissions to allow and deny their access to AWS resources.	**Identity and Access Management** **IBM cloud app ID** --helps developers to easily add authentication to their web and mobile apps with few lines of code,	**Identity and Access Management** - Multi factor authentication -Azure AD Identity Governance - Hybrid Identity Forensics - Managing and securing end-points
Amazon Macie is a security service that uses machine learning to automatically discover, classify, and protect sensitive data in AWS. → protect data in amazon S3	**Multi-cloud Data Encryption** -Role-based access controls -Advanced cryptographic splitting technology -Integrated, certified and KMIP-compatible key management -Object store encryption agent with patented data splitting -RESTful APIs for ease of integration, automation, and scale	**Data Encryption** - Data encryption at rest is available for services across the software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS) cloud models. - Client-side (Azure blobs) and server-side encryption. - Disk encryption - Storage service encryption - Azure SQL, Cosmos DB encryption

Key Management Service, Cloud HSM (hardware security module) → It is a fully-managed service that automates time-consuming administrative tasks for you, such as hardware provisioning, software patching, high-availability, and backups.	**IBM Cloud Key Protect** - Customer-managed Encryption: Customer Root Keys (CRKs) - Flexible - Secure: cloud HMS - Scalable - Application Independence	**Azure key management with key vault** -- Data at rest includes information that resides in persistent storage on physical media, in any digital format. --meet different needs, including file, disk, blob, and table storage -- available across SAAS, PAAS, IAAS
AWS Firewall Manager - security management service that makes it easier to centrally configure and manage AWS WAF rules across your accounts and applications. Using Firewall Manager, you can easily roll out AWS WAF rules for your Application Load Balancers and Amazon CloudFront distributions across accounts in AWS Organizations.	**Security Access Manager** - Securely Adopt Mobile -Establish Identity Federation -Ensure Strong Authentication -Strike a balance between security and usability -Enable risk-based authentication	**Security Access Manager** - Antimalware: Symantec, Trend Micro, McAfee, and Kaspersky - Multi-factor authentication - Express Route - Virtual network gateways - Privileged Identity Management - Identity Protection - Security Center - Intelligent Security Graph
Physical Security → security guards → fencing → security feeds → fire suppression → environmental protection (floods, etc.)	**Physical Security** IBM Cloud data centers are designed to address p**hysical security**. IBM Cloud data center personnel follow strictly-controlled identity and access management policies, including proximity badges and biometrics.	**Physical Security** → tall fences → inside pass two-factor authentication with biometrics → Datacenter floor → only allowed onto the floor that you're approved to enter. → video camera monitoring