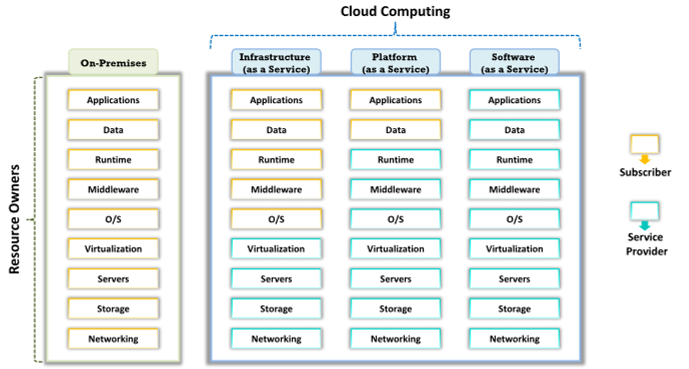
**Module 19: Cloud Computing**

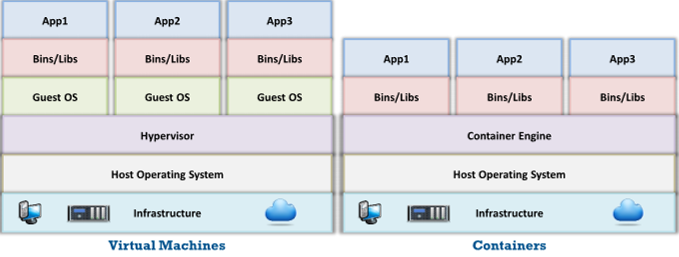
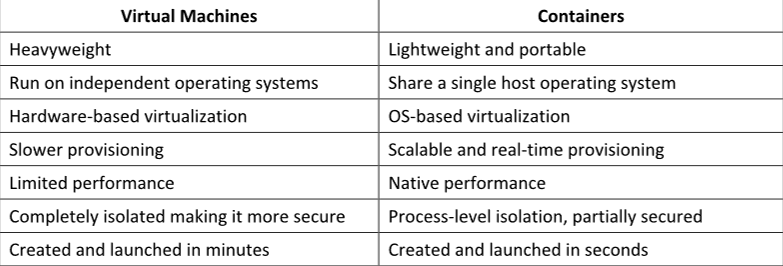
**Concept**

* An on-demand delivery of IT capabilities
* Characteristics of Cloud Computing
  + On-demand self-service
  + Distributed storage
  + Rapid elasticity
  + Automated management
  + Broad network access
  + Resource pooling
  + Measure service
  + Virtualization technology
* Types
  + IaaS (Infrastructure)
    - Provides **virtual machines** and other abstracted hardware and operating systems which may be controlled **through a service API**
    - E.g., Amazon EC2, GoGrid, Microsoft OneDrive, or Rackspace
  + PaaS (Platform)
    - Offers **development tools, configuration management, and deployment platforms** on-demand that can be used by subscribers to **develop custom applications**
    - E.g., Google App Engine, Salesforce, or Microsoft Azure
  + SaaS (Software)
    - Offers **software to subscribers** on-demand **over the Internet**
    - E.g., web-based office applications like Google Docs or Calendar, Salesforce CRM, or FreshbooksFunction
  + IDaaS (Identity)
    - Offers **IAM services** including SSO, MFA, IGA, and intelligence collection
    - E.g., OneLogin, Centrify Identity Service, Microsoft Azure Active Directory, or Okta
  + SECaaS (Security)
    - Provides **penetration testing, authentication, intrusion detection,** anti-malware, security incident, and event management services
    - E.g., eSentire MDR, Switchfast Technologies, OneNeck IT Solutions, or McAfee Managed Security Services
  + Caas (Container)
    - Offers v**irtualization of container engines**, and management of containers, applications, and clusters, through a web portal or API
    - E.g., Amazon AWS EC2, or Google Kubernetes Engine (GKE) END
  + Faas (Function)
    - Provides a platform for developing, running, and managing **application functionalities for microservices**
    - E.g., AWS Lambda, Google Cloud Functions, Microsoft Azure Functions, or Oracle Cloud FnCopyright
* Separation of responsibilities in cloud



* Cloud Deployment models
  + **Public cloud:** Services are rendered over a network that is **open for public use**
  + **Private cloud**: Cloud infrastructure is operated for a **single organization only**
  + **Community cloud:** Shared infrastructure **between several organizations from a specific community** with common concerns (security, compliance, jurisdiction, etc.)
  + **Hybrid cloud: Combination of two or more clouds** (private, community, or public) that remain unique entities but are bound together, thereby offering the benefits of multiple deployment models
  + **Multi cloud:** Dynamic heterogeneous environment that **combines workloads across multiple cloud vendors**, managed via one proprietary interface to achieve long term business goals
* NIST Cloud deployment reference architecture
  + Cloud Consumer
  + Cloud Provider
  + Cloud carrier
  + Cloud Auditor
  + Cloud Broker
* Cloud storage architecture
  + Front-end
  + middleware
  + Back-end
* AI in cloud computing
* VR and Augmented Reality on Cloud
* Cloud service provider
  + AWS
  + Azure
  + GCP (Google cloud platform)
  + IBM Cloud

**Container Technology**

* A package of an **app/software** including all its dependencies such as lib files, configuration files,etc. that run independently of other process in the cloud environment
* Container vs VM
  + VM: **Run multiple OS on a single physical system** and share underlying resources
  + Container: Placed on the top of one physical server and host OS, and **share the OS’s kernel binaries and libs**
  + 
  + 
* **Docker:** An open source technology used for developing, packaging, and runing apps and all its dependencies in the **form of containsers**. It provide a PaaS through **OS-Level virtualization** and delivers containerized software packages
* Docket networking
* **Container Orchestration:** an automated process of managing the lifecycles of software containers and their dynamic environments
* **Kubernetes:** Known as K8s, an open-source, portable, extensible, orchestration platform for managing containerized apps and microservices
* **Container management platforms:** Docxker
* **Kubernetes Platform:** Kubernetes

**Serverless Computing**

* Known as serverless architecture or **FaaS**, is a cloud-based application architecture
* Simply the **process of app deployment** and eliminate the need for managing the server and hardware by the dev
* Serverless computing frameworks: **Azure functions, AWS Lambda**

**Threat**

* OWASP Top10 Cloud Security Risks
  + Accountability and Data ownership
  + User identity federation
  + Regulatory compliance
  + Business continunity and resillency
  + User privacy and secondary usage of data
  + Service and data integration
  + Multi tenacy and physical security
  + Incidence analysis and forensic support
  + Infrastructure security
  + Non-production environment exposure
* OWASP Top10 Serverless Security Risks (**Same with Web Top10**)
* Cloud computing threats
* Cloud attacks: Service hijacking using social engineering, Sniffing
* Cloud attacks: Side channel attacks or Cross-guest VM breaches
* **Wrapping attack:** Attacker duplicates the body of the messages and sends it to the server as a legitimate user
* **MITC attack:** advanced version of MITM attack
* **Cloud hopper attack:** Trigered at the **managed service providers (MSPs)** and their users.
* **Cloud Cryptojacking:** Unauthorized use of the victim’s computer to stealthily mine digital currency.
* **Cloudborne attack:** A vulnerability residing in a bare-metal cloud server that enables the attackers to implant a malicious backdoor in its fireware.

**Cloud Hacking**

* Vulnerability scanning using **Trivy**
* Kubernetes Vulnerability Scanning using **Sysdig**
* Enumerating S3 Buckets
  + S3 is a scalable **cloud storage service** used by **Amazon AWS**
  + Attackers try to find the bucket’s location and name
  + Inspecting HTML
  + Brute-force URL
  + Finding subdomains
  + Reverse IP Search
  + Advanced google hacking
  + Identify open s3 buckets using **S3Scanner**
* Enumerate Kubernetes etcd
  + etcd is a distributed and consistent **key-value storage**
  + Attackers **examine etcd processes**, configuration files, open ports, etc. to identify endpoints connected to the Kubernetes environment
  + **ps -ef | grep apiserve**r is used to identify the location of the etcd server and PKI info
* Enumerate AWS account IDs
* Enumerate IAM roles
* Enumerate bucket permissions using **S3Inspector**
* Exploiting Amazon Cloud Infrastructure using **Nimbostratus**
* Exploiting Misconfigured AWS S3 Buckets
  + Identify s3 buckets
  + Setup aws cmd interface
  + Extract access keys
  + Configure aws-cli
  + Identify vulnerable s3 buckets
  + Exploit s3 buckets
* Compromising AWS IAM Credentials
* Hijacking Misconfigured IAM Roles using **Pacu**
* Cracking AWS Access Keys using **DumpsterDiver**
* Exploiting Docker Containers on AWS using **Cloud Container Attack Tool (CCAT)**
* Gaining Access by Exploiting **SSRF Vulnerability**
* Escalating Privileges of Google Storage Buckets using **GCPBucketBrute**
* Backdooring Docker Images using **dockerscan**
* AWS Hacking Tool: **AWS pwn**

**Cloud Security**

* Cloud security control layer
  + Application
  + Information
  + Management
  + Network
  + Trusted Computing
  + Computation and Storage
  + Physical
* NIST Recommendation for Cloud security
  + **Assess the risk** posed to the client’s data, software and infrastructure
  + Select an appropriate **deployment model** according to the needs
  + Ensure **audit procedures** are in place for data protection and software isolation
  + **Renew SLAs** in case of **security gaps** found between the organization’s security requirements and the cloud provider’s standards
  + Establish appropriate **incident detection** and **reporting mechanisms**
  + Analyze what are the **security objectives** of the organization
  + Enquire about **who is responsibl**e for data privacy and security issues in the cloud
* Zero trust networks:
  + A security implementation that assumes that every user trying to access the network is not a trusted entity by default and verifies every incoming connection before allowing access to the network
  + **Trust no one and validate before providing a cloud service**
* International Cloud Security Organizations: **Cloud Security Alliance (CSA)**
* Cloud Security Tools: **Qualys Cloud Platform**
* Container Security Tools: **Aqua**
* Kubernetes Security Tools: **Kube-bench**
* Serverless Application Security Solutions: **Protego**