



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY
BY EVERYONE'S SMART UNIVERSITY

CompTIA Security+

Lecture 08

SY0-701

Security Architecture

By
Dr. Khaled ELMenshawy

www.midocean.ae

Lecture

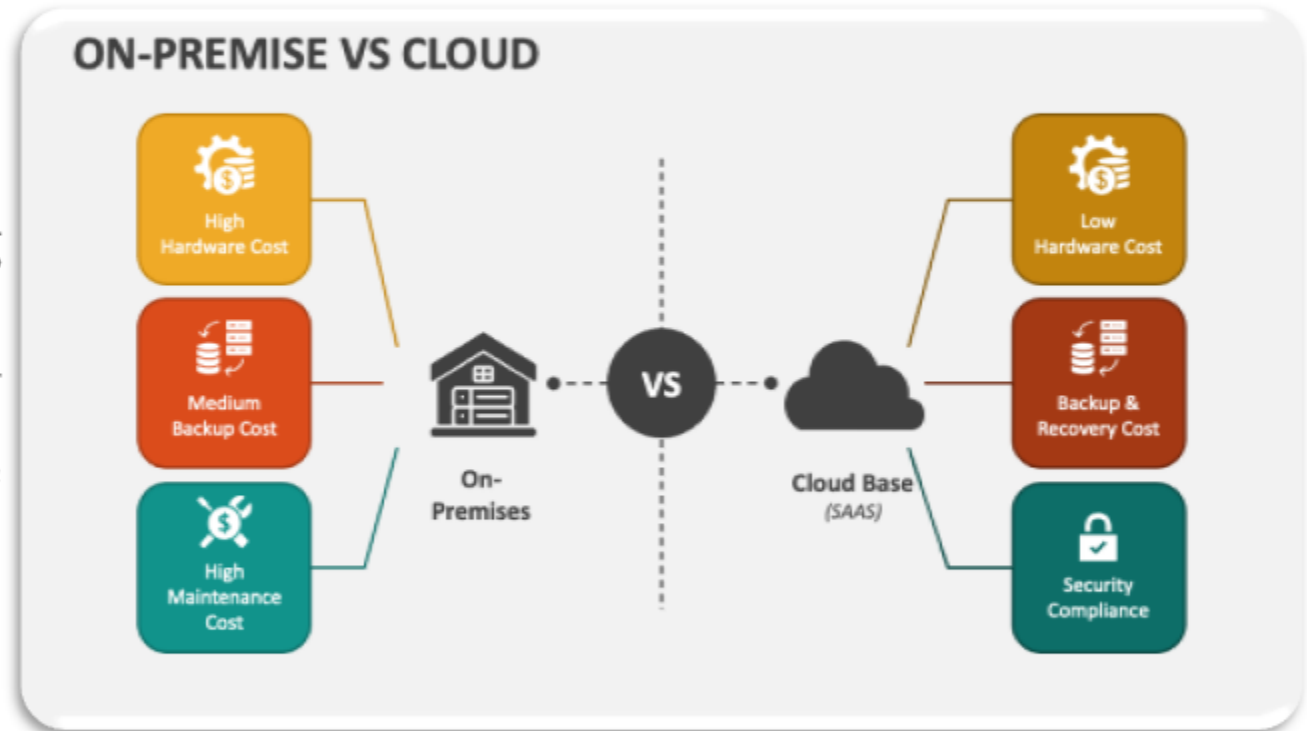
08

LEARNING OUTCOMES

- Differential between On-Premise and cloud computing.
- Understanding the cloud computing.
- Understanding Virtualization.
- Differential between Type I and Type II hypervisor.
- Understanding Containerization.
- Understanding cloud security.
- Understanding Serverless and Microservices.
- Understanding ports and protocols.
- Recognize different port numbers.

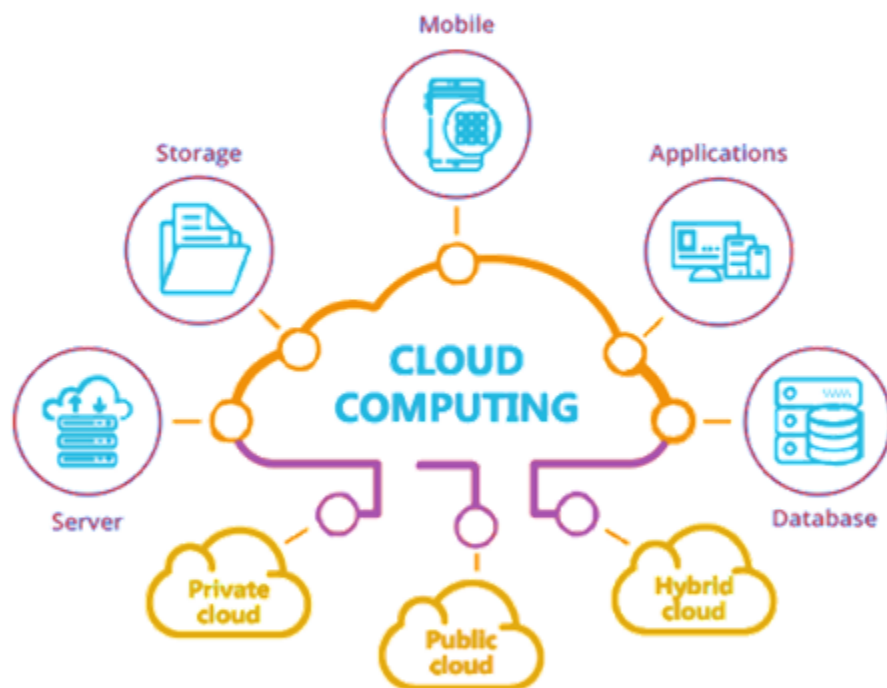
What is On-Premise Solutions?

On-Premise Solutions; is the computing infrastructure that installed and runs on computers that is physically located on site at a business (organization).



What is Cloud Computing?

Cloud Computing; is the *delivery of computing services including servers, storage, databases, networking, software, analytics, and intelligence over the Internet (the cloud)* to offer faster innovation, flexible resources, and economies of scale.



- **Responsibility matrix;** outlines the *division of responsibilities between the cloud service provider and the customer*. **For example;** in an infrastructure as a service (IaaS) model, the provider is responsible for managing the infrastructure while the customer handles everything else including the operating system, middleware, data and applications.
- **Third party vendors;** provide specialized services that *enhance the functionality, security, and efficiency of cloud solutions*. These services range from cloud management tools, security solutions to data analytic tools.

➤ **Hybrid solutions;** *combine on-premise infrastructure, private cloud services, and public cloud services.* They allow businesses to move workloads between environments depending on their needs.

When considering a hybrid solution, *businesses must consider data security, compliance, compatibility and cost.*

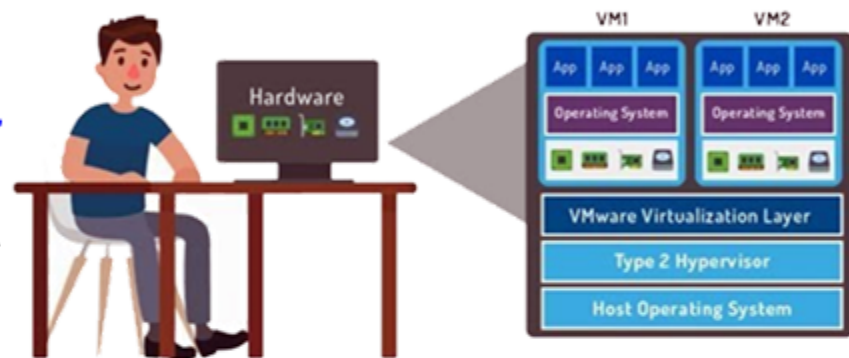
There are some keys that should be consider in cloud computing:

- *Availability*; is the system *ability to be accessed when needed*.
- *Resilience*; is the system *ability to recover from failures and continue to function* due to their distributed and redundant infrastructure.
- *Cost*; is *consider both the immediate and the long-term costs* of cloud adoption.
- *Responsiveness*; is *the speed at which the system can adapt to changes in demand*.
- *Scalability*; is the *system ability to handle increased workloads*.
- *Power*; The cloud service provider takes care of all the infrastructure, including the power supply.

- *Ease of deployment*; cloud services are generally *easier to deploy* than on-premise solutions. They don't require physical installation.
- *Risk transference*; some *risks are transferred to the provider*. However, the customer is still responsible for securing their data and applications.
- *Ease of recovery*; Cloud services often offer *easy data recovery and backup solutions*, protecting businesses from data loss.
- *Patch availability*; Cloud service providers *regularly release patches to fix vulnerabilities*.
- *Compute*; refers to *the number of computational resources that a customer can use*. This includes the number of CPUs, the amount of memory, and the type and size of storage.

What is Virtualization?

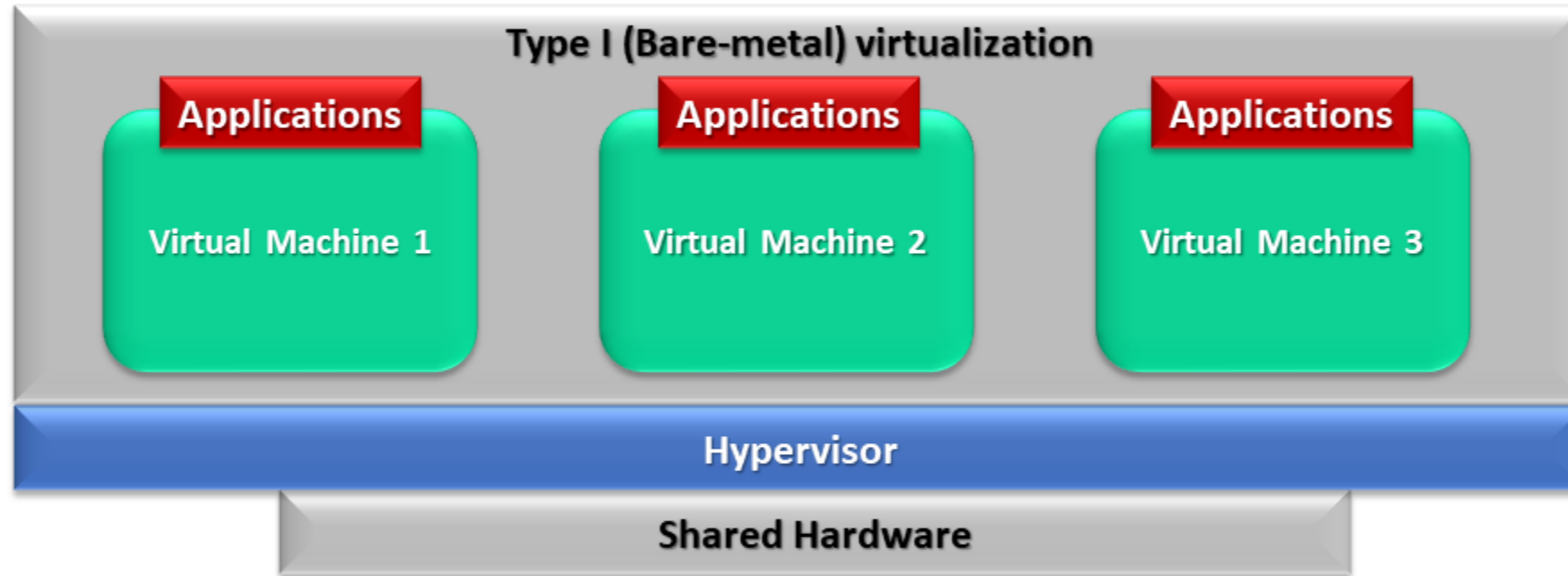
Virtualization; is the *simulation of the software and/or hardware* upon which other software runs. This simulated environment is called virtual machine (VM).



Running *multiple operating systems on the same hardware at the same time* and *Each VM can run its own operating systems and applications* as if it were in a physical machine.

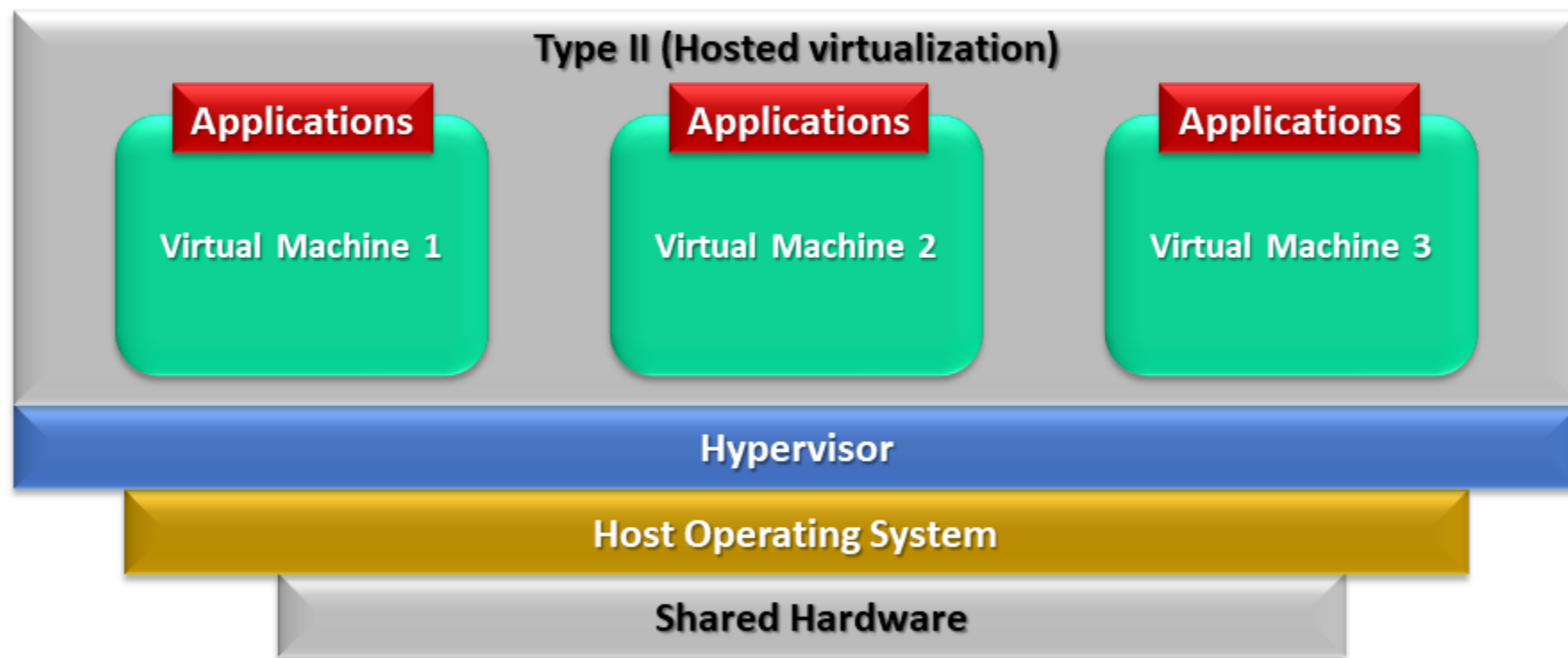
A piece of software called a **hypervisor** is installed to which *manages the distribution of the physical servers' resources* such as the processor, memory, and hard disk space among the virtual machines

Type I Hypervisor



Also known as a ***Bare-Metal*** or a *native hypervisor*, runs directly on the host hardware and functions similarly to an operating system. **Examples of** type 1 hypervisors include Microsoft Hyper-V, Citrix's XenServer and VMware ESXi and vSphere.

Type II Hypervisor

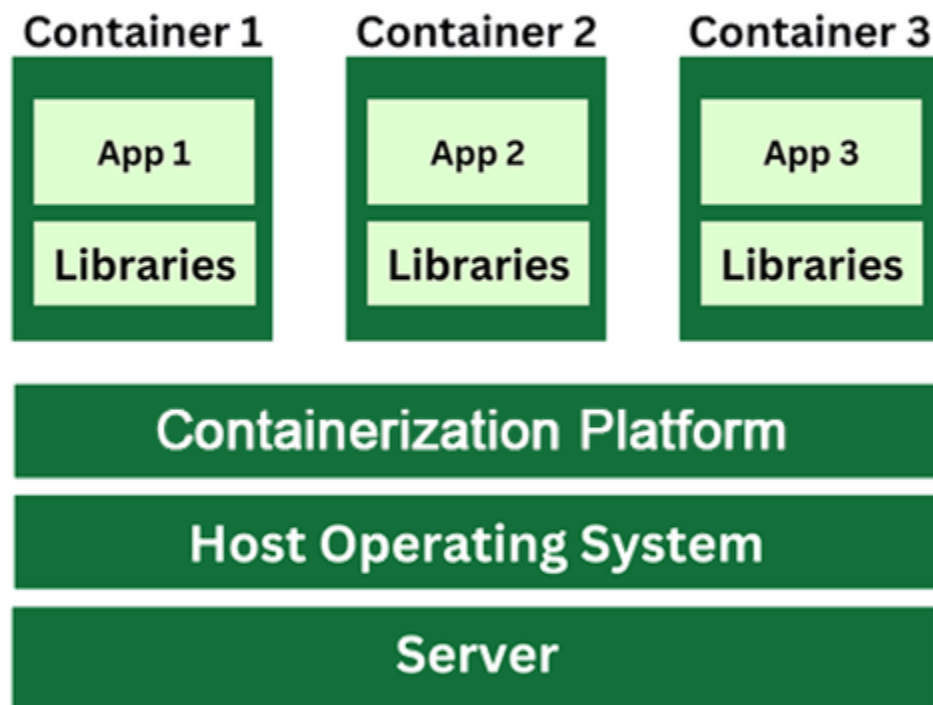


A *Hosted Architecture* which *operates within a standard operating system* such as Windows, Mac, or Linux. *Examples of* type 2 hypervisors include VirtualBox and VMware

Containerization

Containerization; is a software deployment process that *bundles an application's code with all the files and libraries it needs to run* on any infrastructure.

This approach offers several advantages, including *efficiency* and *speed*, *portability*, *scalability*, *isolation*, and *consistency*. Popular containerization technologies include Docker and Red Hat OpenShift.



There are some vulnerabilities that come to virtualization:

➤ *Virtual machine escape*; is breaking out one of isolated virtual machines and *interacting directly with the underlying hypervisor*, then attacker could *migrate themselves out and into another virtual machine* being hosted on the same physical server.

To mitigate VM escape:

- Keep virtual machine software patched.
- Install only the resource-sharing features that you really need.
- Keep software installations to a minimum because each program brings its own vulnerabilities.

- **Privilege elevation**; is occurring when a user is able to *grant themselves the ability to run functions as a higher-level user* such as the root or the administrator.

To mitigate Privilege elevation: Regularly patching and updating software, operating systems, and firmware.

- **Live migration of virtual machines**; is when a *virtual machine needs to move from one physical host to another*. If an attacker can place themselves between these two physical machines, they can implement a form of an *adversary-in-the-middle (AiTM)* attack where they can *capture the data being sent between two physical servers*.

To mitigate AiTM: use strong and unique passwords, enable MFA, and Use conditional access policies.

➤ **Resource reuse**; is a concept in computing where system resources, like memory, storage, or processing power can be reused for different tasks or processes. A resource reuse vulnerability occurs when *a system resource such as memory is not properly cleared or reset before being assigned to another task*. This can potentially *allow sensitive information from the previous task to be exposed to the new task*.

There are some vulnerabilities that come to Cloud Computing:

- **Shared physical server vulnerabilities**; multiple users share the same physical server. This *shared environment can lead to vulnerabilities* if one user's data is compromised, potentially affecting other users on the same server.

To mitigate Shared physical server vulnerabilities:

- Cloud providers should *implement strong isolation mechanisms* such as hypervisor protection.
- Regular vulnerability scanning and patching.
- Network segmentation can help isolate VMs from each other.

➤ *Inadequate virtual environment security*; Virtualization is a cornerstone of cloud computing. However, *inadequate security in the virtual environment* can lead to unauthorized access, data breaches, and other security incidents.

To mitigate Inadequate virtual environment security:

- Secure VM templates.
- Updating and patching VMs.
- Monitoring VMs for unusual activities.

➤ *User access management*; is *unauthorized access to sensitive data and systems*. This is often due to weak passwords, excessive permissions, or lack of user activity monitoring.

To mitigate User access management:

- Implementing strong access control policies.
- Using multi-factor authentication.
- Limiting user permissions based on the principle of least privilege.
- Monitoring user activities for any suspicious behavior.

- *Lack of up-to-date security measures*; Cloud environments are dynamic and constantly evolving making it crucial to *keep security measures up to date*.

To mitigate Lack of up-to-date security measures:

- Regularly updating security measures.
- Regularly reviewing and updating security policies.
- Staying informed about the latest threats and security best practices.

➤ *Single points of failure*; Cloud services often rely on specific resources or processes. *If these fail, it can lead to a complete system outage affecting all users.*

To mitigate Single points of failure:

- Implementing redundancy and failover procedures.
- Regularly testing failover procedures to ensure they work as expected.

➤ *Weak authentication and encryption*; can *allow unauthorized users to gain access to cloud systems*. While weak encryption can *leave data exposed during transmission or storage*.

To mitigate weak authentication and encryption:

- Using multi-factor authentication.
- Strong encryption algorithms.

➤ Unclear policies; refer to the *lack of clear guidelines or procedures for various security aspects* such as data handling, access control, incident response.

To mitigate unclear policies:

- Develop clear, comprehensive security policies that cover all aspects of cloud security.
- Regularly reviewed and updated security policies.
- Regularly training and awareness programs can also help ensure that everyone understands and follows the policies.

➤ **Data remnants**; refer to the *residual data left behind after deletion or erasure processes*.

These data remnants can be a potential security risk as they can be recovered and exploited by malicious actors.

To mitigate Data remnants:

- Implement secure data deletion procedures.
- Managing backups securely.
- verifying that data has been completely removed after deletion.

What is Serverless?

Serverless; is a model where the *responsibility of managing servers, databases, and some application logic is shifted away from the developers.* In a serverless architecture these tasks are handled by cloud service providers.

One of the most popular examples of serverless computing is AWS Lambda, a service offered by Amazon Web Services. With Lambda, developers can run their code without provisioning or managing servers.



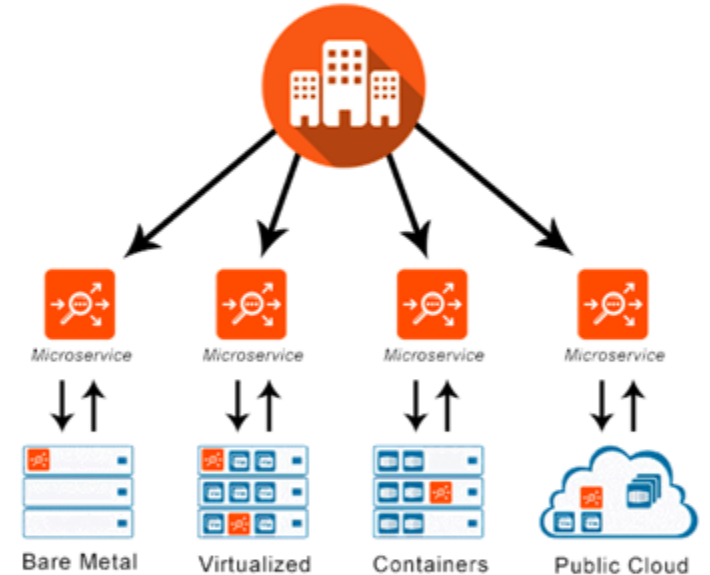
What is Microservices?

Microservices; are a type of software architecture where *large applications are broken down into smaller, independent services*. Each of these services runs a unique process and communicates through a well-defined lightweight mechanism to serve a business goal.

Monolithic
Architecture



Microservices Architecture



Applications

What is Network Infrastructure?

Network Infrastructure; is the separation of network components, which can be achieved either physically or logically.

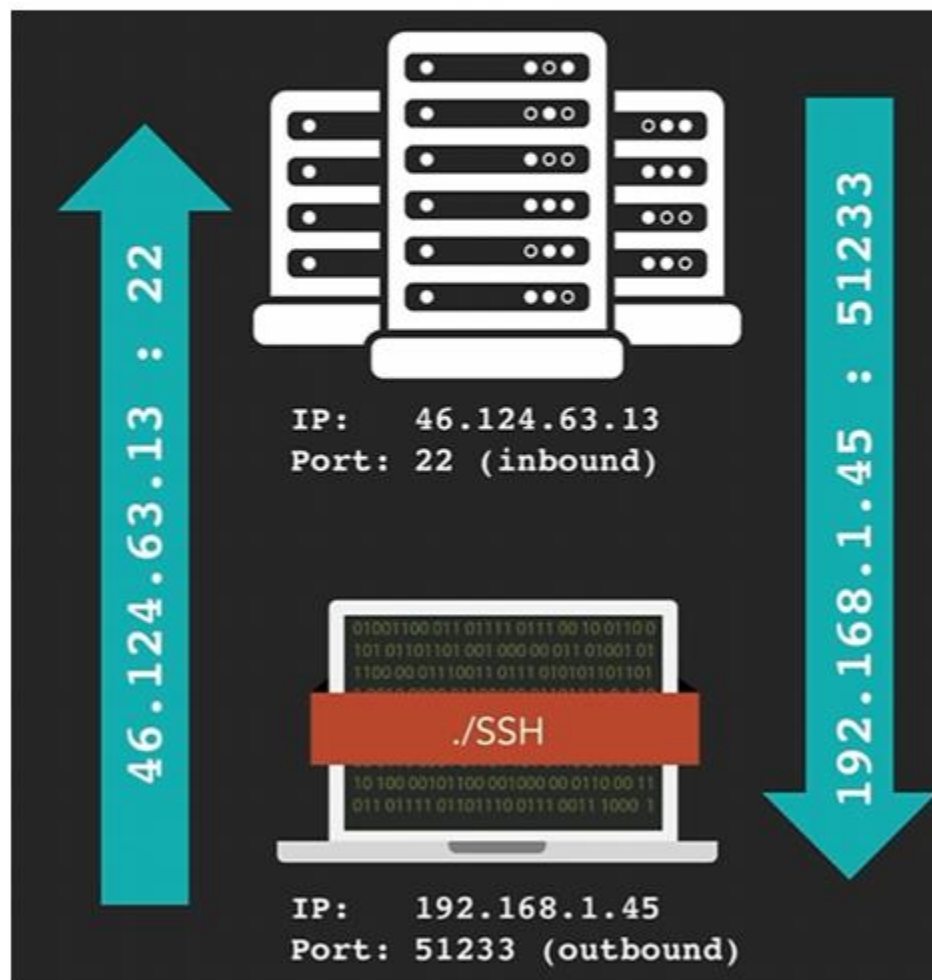


Network Infrastructure

- **Physically separation;** also called *Air Gapping*, is a security measure employed to protect sensitive information. An *Air Gap system is isolated from other networks*, both local and internet.
- **Logically separation;** creating *boundaries within a network that restrict access to certain areas* this is typically achieved through the use of *firewalls, virtual local area networks (VLANs)*, and other network devices that can control traffic based on rules and policies.

Ports:

- **Inbound port;** is used when a computer or server is listening for a connection.
- **Outbound port;** is going to be open by a computer whenever it wants to connect to a given server that is listening.



There is 65535 ports in the network divided as:

- ***Well Known port;*** is *numbered between zero and 1023*. Now these are called well-known ports because they're designated by **IANA**. they're going to be able to assign it to a commonly used port and protocol that everyone can use e.g., https: 443, Telnet : 23.
- ***Registered port;*** is *numbered between 1024 and 49151*. they all have to be used by vendors for their own proprietary protocols e.g., SQL server: 1433, RDP: 3389.
- ***Dynamic and private port;*** is *numbered between 49151 and 65535*. These ports can be used by any application at any time without having to be registered first with IANA.

What is a Protocol?

➤ **Protocols;** is a defined set of rules and conventions that *governs the communication and data exchange between devices or systems* that specifies the format and the sequence of messages that are going to be used for those communications.

➤ As Cybersecurity professional the following *should be memorized*:

- Port Number.
- Protocol used.
- TCP/UDP support.
- Basic description.

Port No.	Connection	Name	Description
21	TCP	File Transfer Protocol (FTP)	Used to transfer files from a host to host.
22	TCP	Secure Shell (SSH)	Provide us with secure remote terminal access.
		Secure Copy Protocol (SCP)	Securely copy files between a local host and a remote host or between two remote hosts
		Secure File Transfer Protocol (SFTP)	Uses secure shell encryption to provide a high level of security for sending and receiving file transfers
23	TCP	Teletype Network (Telnet)	Insecure remote control of another machine using text-based environment.
25	TCP	Simple Mail Transfer Protocol (SMTP)	Responsible for sending emails.
53	TCP/UDP	Domain Name System (DNS)	Used to translate domain names into IP addresses
69	UDP	Trivial File Transfer Protocol (TFTP)	Used with network-based operating systems for sending configuration files or network booting of an operating system.

Port No.	Connection	Name	Description
80	TCP	Hypertext Transfer Protocol (HTTP)	Used for retrieving webpages.
88	TCP	Network Authentication Protocol (Kerberos)	Used for authenticating service requests between trusted hosts across an untrusted network.
110	TCP	Post Office Protocol v 3.0 (POP3)	Used for retrieving email from a mail server.
119	TCP	Network News Transfer Protocol (NNTP)	Used for accessing news groups.
135	TCP/UDP	Remote Procedure Call (RPC)	Used to facilitate the communication between different system processes.
137, 138, 139	TCP/UDP	NetBIOS	Used inside of a Windows domain environment to be able to share things like file and printer in a local Windows environment.
143	TCP	Internet Message Access Protocol (IMAP)	Used for retrieving email from a mail server.

Port No.	Connection	Name	Description
161	UDP	Simple Network Management Protocol (SNMP)	Used to manage network devices.
389	TCP	Lightweight Directory Access Protocol (LDAP)	Facilitate directory services.
443	TCP	Hypertext Transfer Protocol Secure (HTTPS)	Provides a secure web communication process.
456, 587	TCP	Simple Mail Transfer Protocol Secure (SMTPS)	Secure SMTP communications to send our emails.
514	UDP	Syslog	Used for sending log messages.
636	TCP	Lightweight Directory Access Protocol secure (LDAPS)	Used for LDAP Secure over an SSL/TLS connection that is encrypted.
993	TCP	Internet Message Access Protocol over SSL/TLS (IMAPS)	The secure version of IMAP.

Port No.	Connection	Name	Description
995	TCP	Post Office Protocol v 3.0 over SSL/TLS (POP3S)	The secure version of POP3.
1433	TCP	Microsoft SQL server	Facilitate communication with SQL Server.
1645, 1646	TCP	Remote Authentication Dial-In User Service (RADIUS)	Provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service.
1812, 1813	UDP		
3389	TCP	Remote Desktop Protocol (RDP)	Enables remote desktop access.

