**Hypervisor Internals**

An introduction to the use of Hypervisors and their internal components.

# Task – 1

## Introduction

Virtualisation is the concept of creating multiple virtual environments from shared physical hardware. This is achieved by abstracting computing resources and allocating portions of these to the environment. Virtualisation allows multiple operating systems to run on a physical device, where the operating systems do not interact or conflict with each other. These multiple environments are known as **Virtual Machines** (VMs). If you would like to learn more about the concept of virtualisation, visit the Virtualization and Containers room. Hosts that provide virtualisation are known as Hypervisors.

Hypervisors are an old concept in computing. In the 1960s, IBM released the first Hypervisor that provided full virtualisation, the CP-40. Since then, the Hypervisor landscape and virtualisation technology have become sophisticated and even form the backbone of services such as cloud computing. We will discuss this in greater detail in further tasks.

These technologies provide many benefits in a modern IT environment, including:

- Cost Saving
- High Availability
- Easier Management
- Scalability

**Learning Objectives**

- Understand how Hypervisors work, their types, and why they are used
- Discover the Hypervisor landscape
- The application of Hypervisors in a cyber security context
- Become familiar with the internal components of a Hypervisor, as well as how the guest additions that are used to add features to Hypervisors can pose a security risk.

# Task - 2

## Types of Hypervisors

Hypervisors are divided into two categories, which define their position (abstraction) in relation to the hardware of the physical device.

**Type 1 (Bare metal)**

These types of Hypervisors have direct access to a system's physical hardware, don't have to go through another operating system layer (such as Windows or Linux), and are used to run many virtual machines on devices such as servers.

- Performance
- Scalability
- Sophistication

**Type 2 (Hosted)**

These Hypervisors, also known as hosted Hypervisors, differ from bare metal (type 1) Hypervisors because they run on top of an existing operating system (such as Windows or Linux). Hosted Hypervisors are usually found in small environments, such as developers or end-users, where only a small handful of virtual machines are required (such as running Windows on Linux).

- Ease of use
- Free offerings
- Widely Compatible

**What type of Hypervisors have direct access to bare metal?**

**Ans –** type 1

**What type of Hypervisors do not have access to bare metal but run inside and through another Operating System?**

**Ans –** Type 2

# Task - 3

## Hypervisor Landscape

**What is the name of the Hypervisor that can be found as both a type 1 and type 2 Hypervisor?**

**Ans –** Hyper -V

**What is the name of the open-source Hypervisor developed by Oracle?**

**Ans –** Virtual Box

# Task - 4

## Hypervisors in cyber security

Hypervisors have a dominant space in cyber security and can be used in various ways.

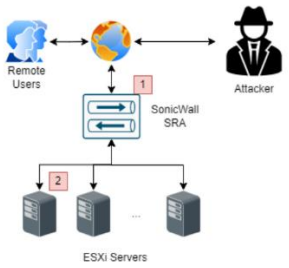
### Security Research

Virtual machines are popular amongst the cyber security community for numerous reasons such as:

- Development
- Analysis
- Research
- Testing
- Pentesting / Red Teaming

### Adversaries

Adversaries and APT groups are increasingly focusing their efforts on Hypervisors because they form the backbone of modern computing today.




**Hypervisor Vulnerabilities**

Hypervisors, like any system, are not without vulnerabilities. Due to the sensitivity and popularity of Hypervisor platforms (especially type 1 Hypervisors), discovered vulnerabilities can pay a handsome reward in various bug bounty programs and the underground market.

For example, at the time of writing, Microsoft offers up to $250,000 for Hyper-V vulnerabilities submitted to its bug bounty program.

**As of the time of writing, what is the maximum amount that Microsoft offers for disclosed Hyper-V vulnerabilities?**

**Ans -** $250,000

**What category of use do cyber security analysts use Hypervisors to analyse malicious code?**

**Ans –** Research

**What is the name of one of the APT groups that has been identified as targeting ESXi Hypervisors?**

**Ans –** AlphaV

# Task 5

## Hypervisor Internals

**What is the acronym for a virtual CPU?**

**Ans** - vCPU

**What is the acronym for a virtual network adapter?**

**Ans** - Vnic

**What virtualisation method allows for a Hypervisor to be ran within a virtual machine?**

**Ans** - Nested virtualisation

# Task - 6

## Guest Additions

**What is the full CVE of the vulnerability that allowed attackers to exploit guest additions to escape the guest environment? Format: CVE-XXXX-XXXX**

**Ans -** CVE-2018-2693

**What name does the VMware guest additions process show up as on the guest?**

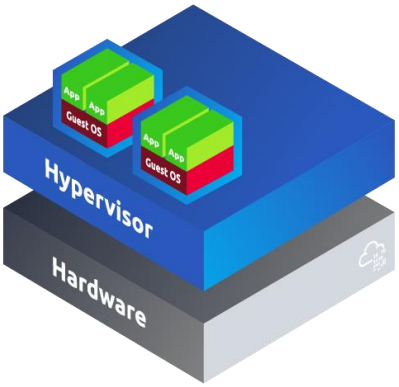
# Task – 7

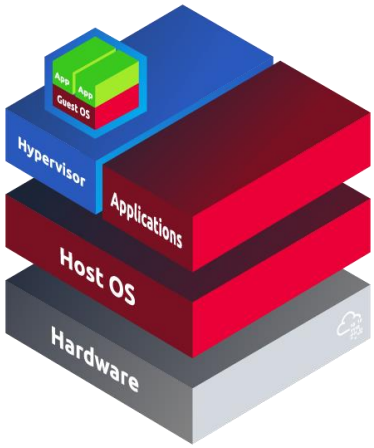
## Practical

objective is to re-create the architecture diagrams for both type 1 and type 2 Hypervisors to reveal a flag.

**What is the flag from the practical?**

Hint (Refer the task 2)




THM{LAYERS_UPON_LAYERS}