Examen module Virtualisation et Architectures de Sécurité

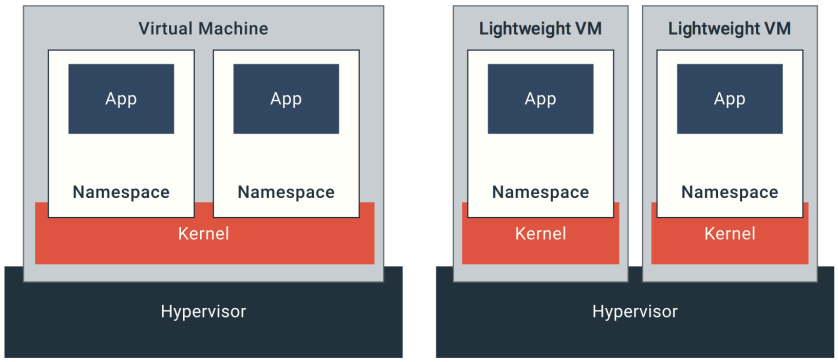
Les documents (notes, slides) sont admis, pas internet !

Questions de cours (0xc points): *Justifiez vos réponses (… brièvement)*

- Q1 - Quel est l'intérêt majeur de la protection SMEP d'Intel ?
- Q2 - Qu'est-ce que la *Nested Virtualization* ?
- Q3 - A quoi servent les *Nested Page Tables* (Intel EPT) ?
- Q4 - Pourquoi Xen et KVM s'appuient en partie sur QEMU ?
- Q5 - De quelle famille (type) d'hyperviseurs fait partie VirtualBox ?
- Q6 - A quoi pourrait correspondre le ring -1 ? Quel composant logiciel pourrait s'y exécuter ?
- Q7 - A l'aide de quel composant est-il possible de se protéger des attaques DMA ?
- Q8 - Comment un *Malware* peut-il tenter de détecter qu'il s'exécute dans une VM ?
- Q9 - Qu'est-ce qu'un noyau d'OS para-virtualisé ?
- QA - Pourquoi la virtualisation matérielle est dite plus performante que l'émulation ?
- QB - Quelle est la différence entre un *systemcall* et un *hypercall* ?
- QC - Quels composants d'un hyperviseur sont susceptibles d'être les plus vulnérables ?

Problème 1 (0x4 points):

Kata Containers is a novel implementation of a lightweight virtual machine that seamlessly integrates within the container ecosystem. Kata Containers are as light and fast as containers and integrate with the container management layers—including popular orchestration tools such as Docker and Kubernetes (k8s)—while also delivering the security advantages of VMs.



Containers in Cloud Today
(Shared kernel, isolation within namespace)

Kata Containers
A lightweight virtual machine isolates each container/pod and provides a separate kernel for each container/pod.

The industry shift to containers presents unique challenges in securing user workloads within multi-tenant environments with a mix of both trusted and untrusted workloads. Kata Containers uses hardware-backed isolation as the boundary for each container or collection of containers in a pod. This approach addresses the security concerns of a shared kernel in a traditional container architecture.

Kata Containers is an excellent fit for both on-demand, event-based deployments such as, continuous integration/continuous delivery, as well as longer running web server applications. Kata also enables an easier transition to containers from traditional virtualized environments with support for legacy guest kernels and device pass through capabilities. Kata Containers delivers enhanced security, scalability and higher resource utilization, while at the same time leading to an overall simplified stack.

Kata Containers Features

Security	Runs in a dedicated kernel, providing isolation of network, I/O and memory and can utilize hardware-enforced isolation with virtualization VT extensions
Compatibility	Supports industry standards including OCI container format, Kubernetes CRI interface, as well as legacy virtualization technologies
Simplicity	Eliminates the requirement for nesting containers inside full blown VMs
Performance	Delivers consistent performance as standard Linux containers

Kata Containers Enables

Multi-tenancy	Event-Driven Container-Native	Increased Resource efficiency	Bridge Ecosystems
Enables multiple tenants to share single container orchestration engine.	Can be launched at anytime without any planning or pre-existing VM cluster requirement.	Small footprint increases density dramatically as compared to traditional VMs.	Utilizes both battle tested hypervisor and bleeding edge container technologies, providing an elegant and cohesive integration.

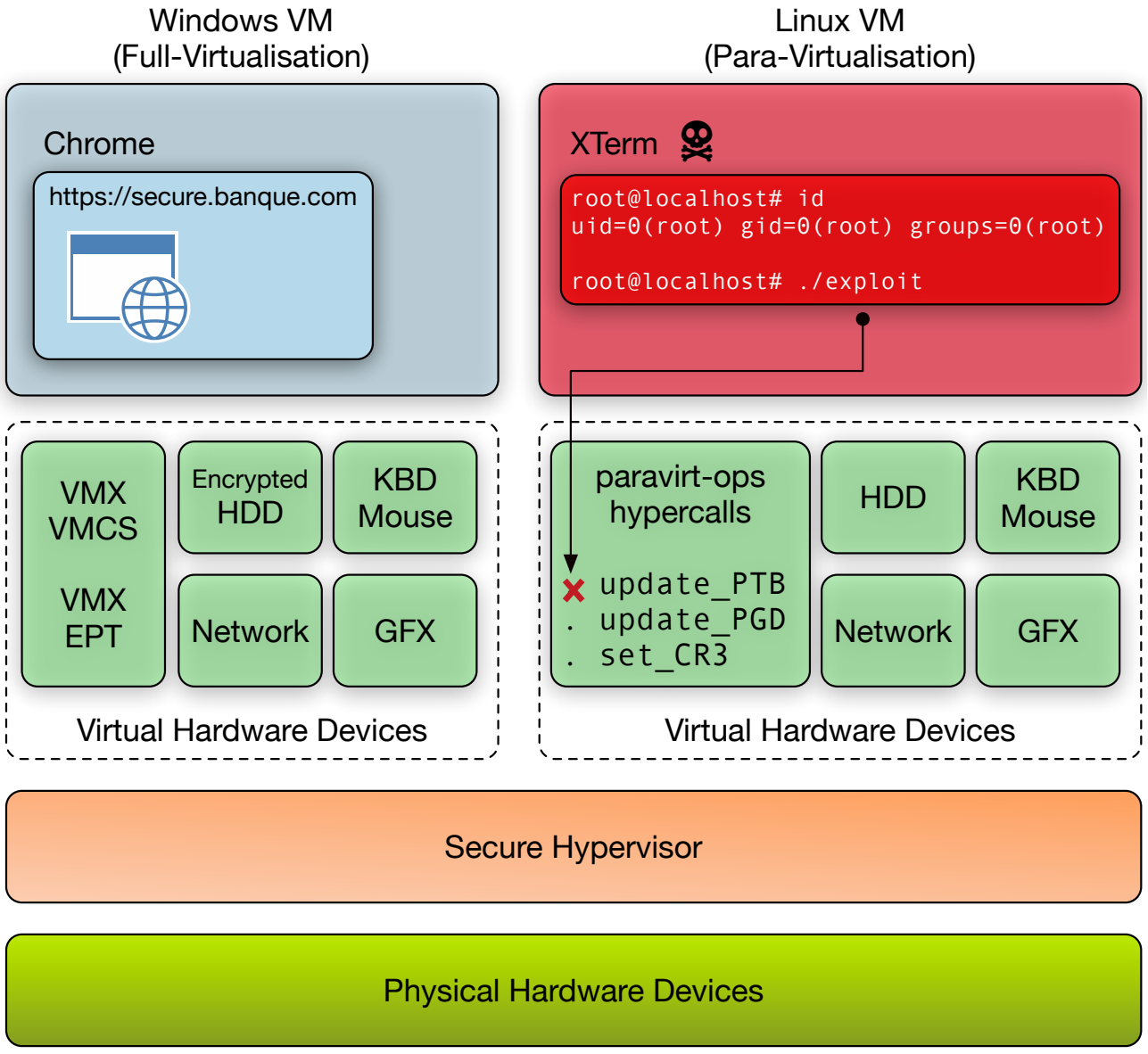
Questions: *Pensez à **justifier systématiquement** mais brièvement vos réponses*

- P1Q1 - Expliquez l'intérêt de la solution *Kata Containers*, par rapport à *Docker*.
- P1Q2 - Quels sont les composants critiques de cette solution ?
- P1Q3 - Quelle stratégie adopteriez-vous pour en évaluer la sécurité ?
- P1Q4 - Quelles peuvent être les implications de sécurité de la phrase « *support for legacy guest kernels and device pass through capabilities* » ?

Problème 2 (0x4 points):

Un gros fournisseur de services dans le Cloud permet d'accéder à des machines virtuelles sécurisées sous Windows et Linux. Ce service est géré par un hyperviseur lui-même très sécurisé, proposant de la virtualisation matérielle dernière génération, ainsi que de la para-virtualisation.

Deux utilisateurs sont actuellement connectés chez le fournisseur: Bob sous Windows qui fait des achats et Alice sous Linux qui ponce le système. Il semblerait qu'Alice ait trouvé une vulnérabilité dans un hypercall critique: `update_PTB`.



Questions: *Pensez à **justifier systématiquement** mais brièvement vos réponses*

- P2Q1 - Au sein de quel composant logiciel se trouve la vulnérabilité ? Est-elle critique ?
- P2Q2 - Alice est-elle en mesure de lancer son attaque ?
- P2Q4 - De quelle manière Alice pourrait exploiter la vulnérabilité ? En quoi pourrait consister l'exploit ?
- P2Q5 - Pensez-vous que Bob court réellement un risque ?