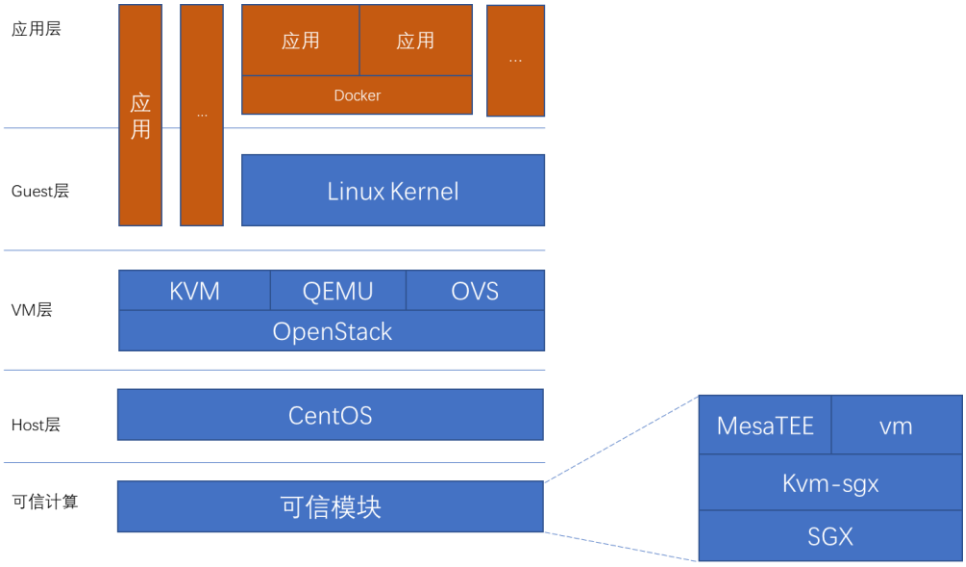
GeekPwn®云安全挑战赛开放赛

技术说明

一、比赛环境

开放赛比赛环境包括标准环境和高防环境，以典型云计算架构进行构建。

*标准环境*软件和版本信息说明如下：



1. 主机层：内核版本是 CentOS7.6 x64 1810.iso 默认安装的 3.10.0

http://isoredirect.centos.org/centos/7/isos/x86_64/CentOS-7-x86_64-DVD-1810.iso

2. 管理层：Openstack Stein，使用 rdo all-in-one 模式进行安装。信息如下：

https://www.rdoproject.org/install/packstack/

Openstack 所有组件(ovs 等)的版本信息如下：

https://releases.openstack.org/stein/index.html

3. 虚拟化层：使用 KVM 作为虚拟化层引擎。

Guest Linux Kernel 版本为 4.4.2

注：本文件中技术信息将持续细化，请留意文件更新

https://cdn.kernel.org/pub/linux/kernel/v4.x/linux-4.4.2.tar.xz

4. 应用层：安装典型应用程序。

例如 redis, elasticsearch，常见数据库等。

安装形式可以是基于 Docker 的形式，也可以是直接安装于虚拟机中。

5. 可信模块是基于 Intel SGX 实现对数据操作的可信执行环境。MesaTEE 通过硬件 TEE 平台，实现了安全的软件栈，版本说明如下：

host-os	ubuntu-18.04.2-desktop-amd64
gust-os	ubuntu-18.04.2-desktop-amd64
kvm-sgx	sgx-v5.0.0-r1
qemu-sgx	sgx-v3.1.0-r1
mesatee	commitid c458bf42c8b44e13ece89050cd4ac7122288616d

代码：https://github.com/mesalock-linux/mesatee

文档说明：https://github.com/mesalock-linux/mesatee/tree/master/docs

*高防环境*是以标准环境配置版本为基础进行针对性加固的云计算环境。

二、攻击环境选择

决赛比赛环境分为标准环境和高防环境，分别代表典型云计算环境、针对性安全加固后的云计算环境。

决赛选手可以根据前期研究情况、自身的技术特点选择一个或多个环境作为攻击目标，获得对应环境中的模块分值，按总积分进行排名。

三、攻击路径选择

各比赛环境中的模块根据挑战难度、利用漏洞（是否 0day）类型等设置不同的分值。比赛不限定选手的攻击路径，决赛选手可以根据自己的技术、掌握的漏洞类型自行设计攻击路径。例如，可以从应用层模块开始向虚拟化层模块突破，也可以从应用层直接突破至宿主机。决赛选手还可以申请快捷路径直达攻击目标模块实施攻击，成功后获得相应积分。