基于云计算和虚拟化的计算机网络攻防实验教学平台建设探索

黄焱

(安徽城市管理职业学院，安徽省合肥市 230011)

[摘 要] 计算机网络实验本来就比较特殊，且破坏性比较大，结构复杂，对各软件性能的要求比较高。基于此，本文从计算机网络攻防实验教学现状入手，对实验教学平台的建设进行了阐述，以供参考。

[关键词] 云计算；计算机网络；教学平台

前言

计算机网络安全实践性很强，加之互联网规模很庞大，涉及到的内容比较多，稍有疏忽就会带来安全隐患，给实验教学带来了很大的挑战。而基于云计算和虚拟化仿真实验为网络实验教学的有效开展提供了新的契机，值得我们去探索和应用。

1 计算机网络攻防实验教学现状

从目前的情况来看，网络安全实验教学与研究工作通常都是在独立的网络环境中进行，借助硬件设备进行实验场景的搭建，或者是运用虚拟仿真技术对真实的网络环境进行模拟。而借助硬件设备开展网络安全实验，对实验室的要求很高，但当攻防实验室对网络结构要求比较复杂时，在实验室中依然不能进行实验。所以，现在的网络攻防实验一般都利用虚拟仿真技术来开展[1]。

现有的关于虚拟仿真技术的攻防教学及培训，对网络安全教学有一定的助推作用，但也存在如下问题：(1)真实网络环境比较复杂，形式多样，仅仅依赖于虚拟化技术设备，无法将复杂的网络拓扑结构、攻防场景模拟出来；(2)无法借助网络展开远程攻防实验，实验设备利用率不高。所以，使用云计算及虚拟技术，开发出能够供广大用户进行远程操作的网络拓扑结构，攻防实验教学平台十分重要。

2 基于云计算和虚拟化的计算机网络攻防实验教学平台建设

2.1 实验平台功能

(1)远程接入控制模块，支持用户经过网络与虚拟仿真平台进行接入；(2)虚拟攻击机云模块，主要借助虚拟化技术，结合实验攻击方式，能够生成各操作系统漏洞的虚拟靶机，按照靶机防护的方案，为虚拟靶机配置各种防护软件。(3)虚拟靶机云模块。借助虚拟化技术，结合实验攻击方式，能够生产配置各类攻击与防护攻击的虚拟机。(4)设备配置扩展模块。允许网络用户为攻击机云平台设置入侵检测等各类硬件设备，建立复杂多样化的网络实验环境。(5)监控中心模块。在进行实验时，自动对平台中的数据流进行捕捉，在实验结束后，网络用户就可以对这些数据薄信息进行下载、分析。(6)管理模块，对用户的平台账户进行添加、维护。(7)实验配置模块。允许用户对攻击机、靶机的地址及结构信息进行配置。(8)教学管理模块。该模块涉及到的功能比较多，可以进行信息的发布、共享、评定等[2]。

2.2 实验平台硬件结构

本文所设计的攻防实验教学平台，其应用服务器主要包含了8台Dell R910，分别与交换机、第一、第二网络云储存相连。其中，第一网络云存储是经过防火墙与交换机相连。防火墙是可以根据自身需要灵活进行选择的设备，能够用别的设备来代替，也可以和交换机直接相连。第一网络云储存存储着具有操作与应用软件漏洞的镜像文件，可以进行Windows、Linux虚拟靶机实例的创建。第二网络云储存与交换机直接相连，储存着已经安装的攻击工具系统镜像文件，借助镜像文件就能够进行Windows、Linux虚拟攻击机的创建。广大网络用户就可以经过VPN网关或交换机相连至虚拟仿真系统[3]。

2.3 实验平台系统架构

网络攻防实验平台是在云计算平台OpenStack开源项目的基础上进行构建的，可以借助该开源项目实现云基础架构服务。实验平台的构建主要运用了OpenStack的Nova实例化虚拟机；Glance提供实例化虚拟机所需的镜像；Cinder提供外接所需的储存服务等等。

实验平台使用控制服务器对各服务器节点进行管理，依据第一、二网络云存储中的镜像，构建虚拟靶机与虚拟攻击机。它们两者间能够利用虚拟网络进行连接，还能够借助网络安全设备与连接设备进行连接，从而使构建的网络环境更加多样化。

2.4 实验平台的维护与流程

在实验平台处在初始化运行阶段时，管理员对账号信息库进行维护，包含用户名、口令等，为账号在第一、二网络云储存中科学地进行磁盘空间的分配，对账户能够操作的实验类别进行指定。

管理员对第一、二网络云存储中的虚拟靶机与攻击机中的镜像文件库、攻击及漏洞库资源进行维护。局部用户只要输入的用户名或口令是正确的，就可以与虚拟仿真系统相连；互联网用户则可以利用VPN与实验平台相连。网络用户连接到这一平台后，就能够运用管理员事先分配好的磁盘空间[4]。

用户可以借助实验类别，根据需要对虚拟攻击机、靶机中的镜像文件进行选择，在相应的磁盘空间中对虚拟实例进行创建，对虚拟实例中的IP地址、网关等等各项应用进行配置，构建虚拟攻击机、靶机的网络连接，在登录至用户所构建的虚拟靶机实例中，借助第一云储存中所配置的安全漏洞软件，让其具有被攻击的环境。同时，借助第二云储存中所配置的攻击机实例，让其具有攻击力。当然，用户可以根据需要在攻击机与靶机实例上设置其他攻击与防护工具。

为了将复杂的网络环境真实的模拟出来，用户可以根据需要设置防火墙，将虚拟靶机或攻击机实力融入到防火墙安全防护范围中，若是遇到风险问题，所配置的攻击就会自动进行网络攻击[5]。

监控中心模块主要是对虚拟攻击机、靶机实例的数据包进行捕捉，对系统操作、及软攻击日志等进行保存。广大网络用户能够对数据包进行下载和查看，对实验结果进行分析。实验结束后，监控中心模块会对长期没有进行任何活动的虚拟攻击机、靶机实例进行自动监控，或直接将其关闭，释放空间。

3 结语

总之，该种计算机网络攻防实验教学平台的构建，有效弥补了传统网络实验教学中存在的不足，为网络安全理论实践教学带来了便利，提高了学生的实践操作能力和水平。

参考文献

[1]李平，毛昌杰，等，开展国家虚拟仿真实验教学中心建设提高高校实验教学信息化水平[J].实验室研究与探索，2015，12(08)：228-229.

[2]万丰，王会林，等，开服务器虚拟技术在实验室信息化建设中的应用[J].实验室科学，2016，8(12)：102-109.

[3]李宗庆，黄永兵，等，一种面向虚拟化云计算平台的内存优化技术[J].计算机学报，2016，5(02)：89-101.

[4]赵威，王海泉，夏春华，面向网络攻防演练的操作系统仿真模拟研究与实现[J].计算机应用研究，2018，7(05)：432-439.

[5]刘卫华，张洪波，等，网络工程虚拟实验室的研究用[J].实验技术与管理，2018，2(05)：222-2259.

作者简介

黄焱，男，出生年月：1985年12月，民族：汉，籍贯：皖金寨县，职称：实验师，学位：工程硕士，工作单位：安徽城市管理职业学院，研究方向：物联网、大数据及软件测试