衡 阳 师 范 学 院

校办通[2018]12 号

衡阳师范学院关于开展 2018 年关键信息基础设施网络安全应急演练的通知

校属各部门：

为深入贯彻习近平总书记关于网络强国的重要思想，进一步提升全社会的网络安全意识和网络安全事件应急处置能力，根据湖南省委网信办、省公安厅《关于开展 2018 年关键信息基础设施网络安全应急演练的通知》（湘网办发[2018]17 号）文件精神，10 月 27 日至 11 月 10 日，省委网信办联合省公安厅将共同组织开展 2018 年关键信息基础设施网络安全应急演练。为做好我校相关工作，现将有关事项通知如下：

一、演练目的

本次网络安全应急演练将采用实战演练的模式，通过组织国内一流网络安全企业的专业技术队伍，对全省范围内的关键信息基础设施进行网络安全实战攻击，即对真实环境下的重要信息系统进行攻防对抗。通过此次网络安全攻防演练，可进一步检验互联网相关参演系统的网络安全保障能力，发现可能存在的网络安全防护、监测和处置措施中存在的短板，积累有效应对网络安全攻击和威胁的经验，提高网络安全的安全防护和应急处置能力。

二、演练安排

此次应急演练过程分为组织阶段、攻防阶段、总结阶段。具体时

间安排如下：

（一）组织阶段：2018 年 10 月 8 日至 10 月 26 日，各部门对本部门信息系统进行网络安全自查和加固。

（二）攻防阶段：从 2018 年 10 月 27 日至 11 月 10 日，共 15 个自然日。攻击时间为每日 8 时到 18 时（含周六、周日）。

演练中的攻击方将从全省范围内的关键信息基础设施中选择部分设施进行深度渗透检测。演练攻击方式包括但不限于 WEB 渗透、内网渗透、钓鱼欺骗、“社会工程学”、无线入侵等。

演练中的被攻击方的主要安全风险包括：目标系统漏洞攻击、边缘系统跳板攻击、内网系统漏洞攻击、内网系统口令爆破等。被攻击方需对演练过程中的攻击行为进行检测、阻断及应急。

（三）总结阶段：2018 年 11 月 28 日，学校对整个应急演练过程进行总结，对演练结果进行评定。

三、工作要求

（一）组织准备

1.学校组织专业队伍应对本次演练，负责学校网络安全保障。并在学校网络安全和信息化领导小组的领导下，做好演练期间的网络安全综合防控及应急处置工作。

2.各部门需高度重视本次应急演练，演练期间（10 月 27 日至 11 月 10 日）须安排专人值班（含周末），并填报《2018 年衡阳师范学院网络安全攻防演练部门值班人员登记表》（见附件 1）。

各部门如有未接入学校站群系统的网络应用系统，须确定参加本次演练的信息系统管理员名单，并填报《2018 年衡阳师范学院网络安全攻防演练重要信息系统情况登记表》（见附件 2）。

各部门值班人员和信息系统管理员须密切关注本部门的网站及网络应用系统，如发现异常，应即时报告学校网络安全和信息化领导小组办公室（联系电话：8486636,3456023）。

3. 各部门须在10月26日下午五点之前将《2018年衡阳师范学院网络安全攻防演练部门值班人员登记表》和《2018年衡阳师范学院网络安全攻防演练重要信息系统情况登记表》报送学校网络安全和信息化领导小组办公室（计算机楼105室）。

（二）资产梳理和安全自查

信息与网络中心组织技术人员在10月27日前协同各二级学院、各部门信息系统管理员对本单位网络应用系统进行互联网资产自查、网络路径梳理、关联系统资产梳理、安全漏洞扫描、安全基线检查等工作。

（三）安全加固和整改

1. 信息与网络中心针对资产梳理和安全自查结果,采用防火墙安全策略优化、日志审计、主机加固等措施及时对系统漏洞隐患进行加固，修订、优化网络安全策略配置，加强安全措施效能发挥，降低可能被外部攻击利用的脆弱性和风险。

2.学校行政办公区域与机房上网用户须对联网计算机进行以下处置工作：

（1）即日起至演练结束，确保已经将计算机操作系统及其最新补丁、防病毒软件、软件防火墙等防护软件升级到最新版本（建议使用360安全卫士进行系统补丁的更新），同时严禁将不安全的计算机设备接入网络。

（2）所有计算机终端，在完成操作系统更新、安装最新补丁之前，严禁使用U盘、移动硬盘等可执行摆渡攻击的设备。

（3）用户一旦发现系统或网络异常，请立即断网（拔掉网线、关闭无线网卡或断开无线连接、关机等），同时请告知信息与网络中心。

（4）尽可能停止使用 Windows XP，Office2003、Office2007等微软已不再提供安全更新的操作系统和应用软件。建议使用 Windows 7，Office2010。

（5）用户必须将联网计算机的用户密码进行修改加固，可使用8位以上的大写+小写+数字+特殊字符做为新密码。如发现来源不明的邮件、网络文件或图片时，请在确认安全前不要打开。

3.完善应急机制

网络安全与信息化领导小组办公室修改完善学校网络安全事件应急处置流程和预案，完善内部应急响应机制，明确职责分工，推演系统各节点被攻破后的紧急处置措施，提高学校对网络安全事件的应急处置能力。

（四）演练防护

学校组织相关网络与系统管理人员在演练期间持续对网络攻击进行监测并及时阻断，针对演练中发现的漏洞和弱点，及时进行修补加固，积极应对，协同进行安全处置。

1.业务监测

信息与网络中心协同各部门实时监测应用系统和服务器运行状态，包括系统访问是否正常、业务数据是否有异常变更、系统目录是否出现可疑文件、服务器是否有异常访问和修改等。

2.攻击监测和阻断

演练过程中，信息与网络中心应充分利用现有安全设备（防火墙、日志审计、流量监控等）实时监测网络攻击行为，详细记录攻击相关数据；依据攻击行为的具体特点制定攻击阻断的安全措施，详细记录攻击阻断操作。

3.应急处置

在演练过程中，经分析确定已发生网络攻击，且攻击已成功进入系统、获取部分权限、上传后门程序，应立即启动应急响应预案，按《衡阳师范学院网络安全事件应急处置流程图》进行处置（见附件2）

在网络攻击事件处置完毕后，应针对攻击所利用的安全漏洞或缺陷，组织技术力量尽快进行漏洞修复和问题整改。

（五）总结汇报

学校将全面总结本次攻防演练的工作情况，包括组织队伍、攻击情况、防守情况、安全防护措施、监测手段、响应和协同处置等，形成总结报告并向上级部门汇报。

附件：

1. 2018 年衡阳师范学院网络安全攻防演练部门值班人员登记表
2. 2018 年衡阳师范学院网络安全攻防演练重要信息系统情况登记表
3. 衡阳师范学院网络安全事件应急处置流程图

衡阳师范学院办公室

2018 年 10 月 24 日

附件 1：

2018 年衡阳师范学院网络安全攻防演练部门值班人员登记表

部门（签章）：　　填表时间：　　年　　月　　日

部门	值班人员	值班日期

备注：此表纸质稿送交：信息与网络中心尹军，18073417318，计算机楼 105 室。

电子稿发送至邮箱：yinjun@hynu.edu.cn

附件 2：

2018 年衡阳师范学院网络安全攻防演练重要信息系统情况登记表

部门（签章）： **填表时间：** 年 月 日

序号	部门	信息系统名称	域名	IP 地址	管理员信息（含姓名、联系电话、QQ 号、微信号）	部门负责人

备注：此表纸质稿送交：信息与网络中心尹军，18073417318，计算机楼 105 室。

电子稿发送至邮箱：yinjun@hynu.edu.cn

附件 3：**衡阳师范学院网络安全事件应急处置流程图**