攻防演练任务分工

**一、前期准备工作**

为有效开展网络安全攻防演习，检验安全防护体系和应急响应流程的有效性，同时避免攻防演习影响业务系统和网络系统正常运行，需要各单位联合系统的维保公司完成以下准备工作：

1、信息系统自查工作

（1）检查信息系统账号及密码管理

a）满足密码复杂性要求：密码长度至少8个字符；密码至少包含4类字符中3类字符（英语大写字母、英语小写字母、数字、特殊字符）；

b）设置无效登录的次数，如登录失败5次锁定账户；

c）设置口令复杂度校验机制，当密码不符合复杂度要求时无法使用；

d）重命名或者禁用系统默认账户；

e）及时终止离岗人员的所有权限，删除离岗人员账号；

f）不应该存在共用账号的情况；

g）授予不同的账户为完成各自承担任务所需的最小权限，即根据岗位职责，为不同岗位的工作人员设置不同等级的权限。（如信息中心数据库安全审计系统根据不同岗位职责划分不同权限，只有网络安全部科长肖刚拥有该系统超级管理员权限，负责网络安全的乔玲只拥有该系统中安全功能相关的权限，负责网络管理的赵冉只拥有该系统中审计功能相关的权限。）

（2）检查服务器和系统安全

a）及时更新操作系统和数据库，确保无已知漏洞；

b）限制服务器远程管理的接入地址，仅允许特定的地址访问或者仅允许通过堡垒机进行远程管理；

（3）信息系统应使用https协议，防止鉴别信息在网络传输过程中被窃听。如未使用可向信息中心申请证书，在服务器上进行部署。

2、信息系统备份工作

（1） 确保信息系统的数据可以备份，并且备份文件应该至少保存3个月；

（2）提前备份重要数据，在遇到紧急情况时，可以实现数据和系统的恢复；

（3）根据数据的重要程度采取多样化的备份方式。如开外网的信息系统的业务数据采取异地容灾备份，对于其他信息系统业务数据采取本地或者异机备份；

3、信息中心做好网络安全检测

（1）确认Web应用防护系统、入侵防御系统、防火墙等网络安全设备有效运行，调整并优化访问控制策略和拦截策略，并将特征库和病毒库更新到最新版本；

（2）梳理信息系统中开外网的端口号所对应的具体业务，在防火墙上关闭不必要的端口；

（3）在核心交换机华为16808上基于vlan对135，139，445，3389，5938，888,2222等公共端口进行访问控制，禁止任何用户访问服务器的相关公共端口；

（4）进一步限制VPN账号的访问权限，避免越权访问的行为，即普通师生不应该拥有访问信息系统服务器和数据库的权限，公司人员只拥有访问其搭建的信息系统的服务器和数据库的权限；

4、技术人员准备：根据各单位情况协调技术人员，确认在演习过程中运维人员就位，必要时可协调系统开发单位和设备厂商人员；

5、制定应急预案：为了防止演习中发生不可控突发事件导致业务不能正常运行，各二级单位应制定应急处理预案，预先对可能发生的紧急事件做出处置安排措施。具体制定可参考滁州学院网络与信息安全突发事件应急预案。

**二、演练过程中工作**

1、攻防演练期间，各二级单位信息员和信息系统（网站）负责人每隔1个小时监测信息系统（网站）运行状况。各二级单位信息员每天中午12:00前将本单位网络安全情况报送至电子邮箱jolin\_qiao@chzu.edu.cn，并保持通讯畅通。

（1）查看系统界面是否被篡改；

（2）查看信息系统的主要功能是否可以正常使用

（3）联系信息系统运维人员查看系统日志（登录日志和操作日志）是否存在异常登录和操作情况；

2、各二级单位一旦发现信息系统（网站）异常，第一时间启动应急预案，及时向信息中心通报情况，根据不同的事件类型和事件级别，采取科学有效的应急处置措施，尽最大努力将影响降到最低。

3、信息中心对负责的信息系统开展上述工作。同时，在攻防演练期间在Web应用防护系统、入侵检测系统和防火墙等网络安全设备中设置高级防护策略，并且每隔1个小时查看网络安全设备的情况，及时跟踪和拦截恶意攻击，并将恶意地址加入黑名单。同时，在晚上19:00到第二天早上7:00，在网络安全设备上开启高强度防护，进一步阻断恶意攻击。

**三、演练结束后工作**

1、信息中心根据攻击方提供的演练成果，进行汇总与分类。

2、信息中心根据分类情况，将信息系统中存在的相关漏洞信息以纸质版整改通知的形式，发送给负责该信息系统的信息化负责人，并签署签收表。同时提醒信息化负责人，对于存在问题的信息系统，在总结会议上汇报应急处置措施和过程。

3、各二级单位收到整改通知后，积极联系系统运维人员，必要时联系厂商，对于系统中存在的漏洞，及时修复。二级单位信息化负责人在总结会上对于发现的问题，汇报应急处置措施和过程。

如在攻防演练期间遇到问题，请联系信息中心乔玲（0550-3510264）及时反馈。