**浙江大学安全攻防演练工作方案**

此次攻防演练工作由浙江大学网络与信息安全领导小组牵头组织，信息技术中心和专业安全公司做技术支持，各单位同步配合共同完成。攻防演练过程主要是由网络安全攻击组通过安全扫描、攻击渗透测试，发现各业务系统薄弱风险点，各单位协同运维厂商、开发厂商等成立攻防演练防守组统筹防御，加强系统防护、监测及处置工作。

工作方案具体内容如下：

1. **演练工作组织架构**

针对本次攻防演练工作组织架构如下：

1. **领导指挥组**

由浙江大学网络与信息安全领导小组担任，主要负责指挥攻防演练活动整体过程、确定支撑单位、明确各组工作职责。

1. **专项工作组**

由网络与信息安全领导小组办公室、信息中心担任，主要负责攻防演练工作统筹协调，组织协调业务部门、支撑单位（包括安全厂商、运维厂商、开发厂商等）落实具体方案制定、攻防人员安排、具体工作落实、落实漏洞报告评分及漏洞通报下发工作。

1. **攻击组**

由浙江大学信息中心人员、专业安全公司派驻技术人员成立攻击组。负责正式攻防演练期间对参演网站系统的攻击得分。

1. **防守组组**

由各单位、各部门、各学院的业务部门提供支持，各运维厂商、开发厂商配合。主要负责攻防演练期间的防护措施落实和加强，以及在正式攻防演练期间监测攻击行为和抵御处置。

1. **选择参演对象**

本次攻防演练报送的业务系统作为防护和被攻击对象。参演系统为全校登记在册的所有网站和信息系统（限校网内部署的）。

1. **演练期间攻与防及评分细则**

**（一）攻**

由攻击组的工程师负责。在攻击动作允许的范围内，针对分配的攻击对象，根据攻击得分规则，派遣优势力量优先测试得分高的点，尽可能多得分。

根据得分点编写攻击测试简报，统一交由浙大信息中心进行下发整改。

攻击评分标准：

漏洞发现类评分

|  |  |  |  |
| --- | --- | --- | --- |
| **类型** | **威胁类型** | **赋值规则** | **备注** |
| 漏洞风险发现 | 低危风险漏洞 | 2分/1个 | 裁判依据提交的漏洞情况，评判漏洞是否真实存在，及漏洞影响程度进行评分，累计得分 |
| 中危风险漏洞 | 5分/1个 | 裁判依据提交的漏洞情况，评判漏洞是否真实存在，及漏洞影响程度进行评分，累计得分 |
| 高危风险漏洞 | 10分/1个 | 裁判依据提交的漏洞情况，评判漏洞是否真实存在，及漏洞影响程度进行评分，累计得分 |
| **口令类** | 弱口令/口令泄露 | 5分/1个8分/1个 | 1、根据提交口令核实后，普通用户5分，同一系统不累计2、管理员8分/个 |
| **权限类** | getshell | 50分/1个 | 裁判依据提交的漏洞情况，评判漏洞是否真实存在，及漏洞影响程度进行评分，累计得分 |
| **其他** | 大规模信息泄露、数据泄露 | 10分/个 | 数据50条以上且可以与上述中高危累计得分 |

发现演习前已有攻击事件类评分

|  |  |  |  |
| --- | --- | --- | --- |
| **类型** | **威胁类型** | **赋值规则** | **备注** |
| 发现演习前已有攻击事件 | 演习前发现目标系统网络中已被植入webshell木马、主机木马 | 10-50分/个主机，根据木马发现的网络重要性给分 | 提供包含确凿证据的详细分析报告，由裁判组研判后给分，累计得分 |
| 发现其他系统被控制的线索情况 | / | 由裁判核定给分，累计得分 |

注：重复漏洞不得分。禁止破坏性测试

注：专项组根据评分规则，逐个验证攻击成果并打分

**（二）防**

在正式攻防演练期间，主要体现各监测各院校监测能力、应急处置能力。由各单位、各部门、各学院协调各自安全厂商、运维厂商、开发厂商等共同配合，开展以下工作内容：

1、每天演练开始（9：00）前，各单位负责确认各参演业务系统的运行情况巡检，确保系统有效运行。

2、每天演练结束（17：00），各单位分工根据攻击监测到行为进行分析，汇总攻击和阻断情况，并每日提交防守处置报告，发送邮件到sec2018@zju.edu.cn。

3、在演练期间，实时监视网站（系统）访问日志和流量，分析检测到的攻击行为，确定攻击来源、攻击手段、攻击真实性等，确定为攻击行为后，写入报告提交。对于部分单位有独立安全防护设备的系统，由运维厂商及时通过防火墙、WAF等防护设施采取阻断措施，并写入报告提交。

4、在演练期间，追溯检测到的攻击源，对于上传木马后门、权限获取、弱口令爆破等行为及时阻断和清查，并及时修补可被利用的安全漏洞，处置过程写入报告提交。

5、在演练期间，实时监视参演系统服务器、应用程序的运行情况，发现系统异常，即使采取针对性的应急处置预案，进行恢复，处置过程并写入报告提交。

6、在演练期间，接到演练指挥中心的应急事件通报，即可启动应急处理流程，包括（1）立刻验证通报是否属实，确定属实即可断网（因为是演练就不用断网了），通知演练指挥中心。（2）确认后，立即向上级主管负责人汇报。（3）组织运维人员，即可分析日志，追踪溯源，查找原因，封堵漏洞，并写出事件分析报告。（4）组织运维、开发人员恢复系统，恢复上线，并上报演练指挥中心。

按照防守方提供的防守报告进行核定加分，按照攻击方提供的攻击成果进行减分，由专项工作组依据赋分标准、赋分规则进行评分，逐项打分，总分为各分项之和。

防守评分标准：

|  |  |  |  |
| --- | --- | --- | --- |
| 工作阶段 | 赋分标准 | 赋分规则 | 备注 |
| 监测发现能力 | 及时发现存在的威胁，并提供威胁ip地址，问题分析详细，定位准确。 | 分为优、良、中、差四个级别，优得30分；良得20分；中得10分；差得0分 | 提交问题监测报告，由专项工作组核定给分 |
| 应急处置能力 | 针对发现的威胁积极应对，配合有效固定证据并快速有效处置  | 分为优、良、中、差四个级别，优得30分；良得20分；中得10分；差得0分 | 提交应急响应工作报告，由专项工作组核定给分 |

|  |  |  |  |
| --- | --- | --- | --- |
| 减分项 | 赋分标准 | 赋分规则 | 备注 |
| 攻击成果 | 按照攻击方提供的攻击成果进行减分 | 攻击成果加多少分，防守系统扣除多少分。 |  |

1. **时间安排**

**演练整体流程计划**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **任务** | **开始时间** | **结束时间** | **参与方** |
|  | 演练前动员大会 | 9月16日 |  | 各单位网络安全负责人、安全员 |
|  | 演练期间攻与防 | 9月16日 | 9月20日 | 安全小组、专业安全公司、各单位安全员、开发商、运维商 |
|  | 总结及整改落实 | 9月23日 | 9月27日 | 各下级单位落实整改 |

1. **应急预案**
	1. 应急处理

针对此次演练可能出现的突发情况，制定本次演练期间应急处置措施。

应急工作小组在应急处置工作中应通过口头、电话、或书面方式定时向上级应急部门汇报应急处置工作进展情况。网络安全事件应急处理过程中根据不同事件类型采取以下应急处理措施：

**（1）有害程序事件**

①中断感染主机的网络连接；

②查杀恶意程序；

③升级系统，安装系统补丁；

④安装和升级防病毒软件。

**（2）网络攻击事件**

①确定攻击来源，攻击对象，影响范围；

②判断攻击后果，根据影响程度决定是否需要紧急切断服务器的网络连接，以保护重要数据及信息；

③在边界防火墙、入侵防御设备上对来源IP地址进行阻断；

④评估系统受损程度，备份系统、保存系统日志，分析攻击手段、攻击使用漏洞、攻击过程和追溯源地址；

⑤恢复被攻击系统，安装系统补丁，升级系统。

**（3）信息破坏事件**

①及时从备份数据中恢复受破坏的最新信息数据；

②检查恢复后的系统状态是否正常运行；

③分析信息数据受破坏的原因，人为恶意破坏的应进行追溯，系统故障导致的应分析系统软件故障点，及时联系软件开发商进行修复。

**（4）信息内容安全事件**

①暂时切断网站对外服务；

②网站维护人员即刻登录后台，上传换回原始页面；

③网站、网页由安全监控平台随时密切监视信息内容；

④保存有关日志审计记录；

⑤备份不良信息出现的目录。

**（5）设备设施故障事件**

①分析、确认故障设备，准确定位设备位置；

②切换备用设备；

③联系设备供应商分析设备故障原因，及时进行修理，涉外修理的应清理数据；

④无法修理的应采购新的设备，保证设备冗余状态。

* 1. 结束响应

网络安全事件经应急处置后，判断是属于主动行为还是被动、无意的行为及造成的危害程度，得到有效控制，事态下降到一定程度或基本得到以解决，将各监测统计数据上报应急领导小组，批准同意后，应急结束。并转向后续工作。

* 1. 系统恢复

应急处置完毕后，信息系统恢复重建工作按照“谁主管谁负责，谁运行谁负责”的原则，由事发业务系统负责单位组织制定恢复、整改或重建方案。

附件：渗透结果总结汇总如下表

|  |  |  |  |
| --- | --- | --- | --- |
| **渗透系统对象** | **漏洞类型及** | **URL（可罗列）** | **数量** |
| 门户网站http://abc.com | SQL注入 | <http://IP/list.php?id=132><http://IP/list.php?id=132><http://IP/list.php?id=132> | 3 |
|  |  |  |
| 邮箱系统http://mail.abc.com | 弱密码 | 账户名/密码1账户名/密码2.... | 10 |
|  |  |  |
|  |  |  |

附件、渗透分析过程

（一）渗透路径说明

1、路径（写至最深区域为止，一次即可）

互联网xxx系统（域名，ip地址）——>内网xxx系统（域名，ip地址）——>专网xxx系统（域名，ip地址）

2、路径截图

路径截图

（二）渗透成果说明

1、成果一

1）、成果目标基本情况

目标业务系统名称、域名、url、ip地址等。

2）、成果说明

I、漏洞情况及控制权限说明

II、放置webshell、木马等其它工具详细路径等说明

描述通过什么漏洞、什么方法获取了什么权限。

III、添加账号信息说明

描述添加的应用账号、主机账号等信息。

IV、其它攻击信息说明

3）、成果截图

2、成果二

。。。

附件：防守汇总报告模板

1. 系统名称

域名：XXX

系统名称：XXX

1. 结果综述

当日防守整体情况,如发现入侵情况、成功拦截处置整体状况

1. 防守过程

发现攻击队IP进行XXX攻击测试等，发现的问题及处理方法等

截图：。。。。。。