攻防演练行动

专项应急演练方案

文件编号	
现 版 本 号	V1.0
实施日期	

xxx 信息中心

目录

1 演练概况

1.1 演练目的

本次应急演练，通过实施具体场景，旨在保障“护网行动”攻防演习期间各应急小组协调组织能力， 提升攻防演习期间对安全问题的应急响应水平以及网络安全预警时效。完善演练预案、改进应急操作及流程。

1.2 演练时间

正式演练： x 月 xx 日 09:30-10:00

演练总结： x 月 xx 日 10:00-10:30

1.3 演练角色

演练指挥： xx

攻击方： xxxx

防守方：本次应急响应小组

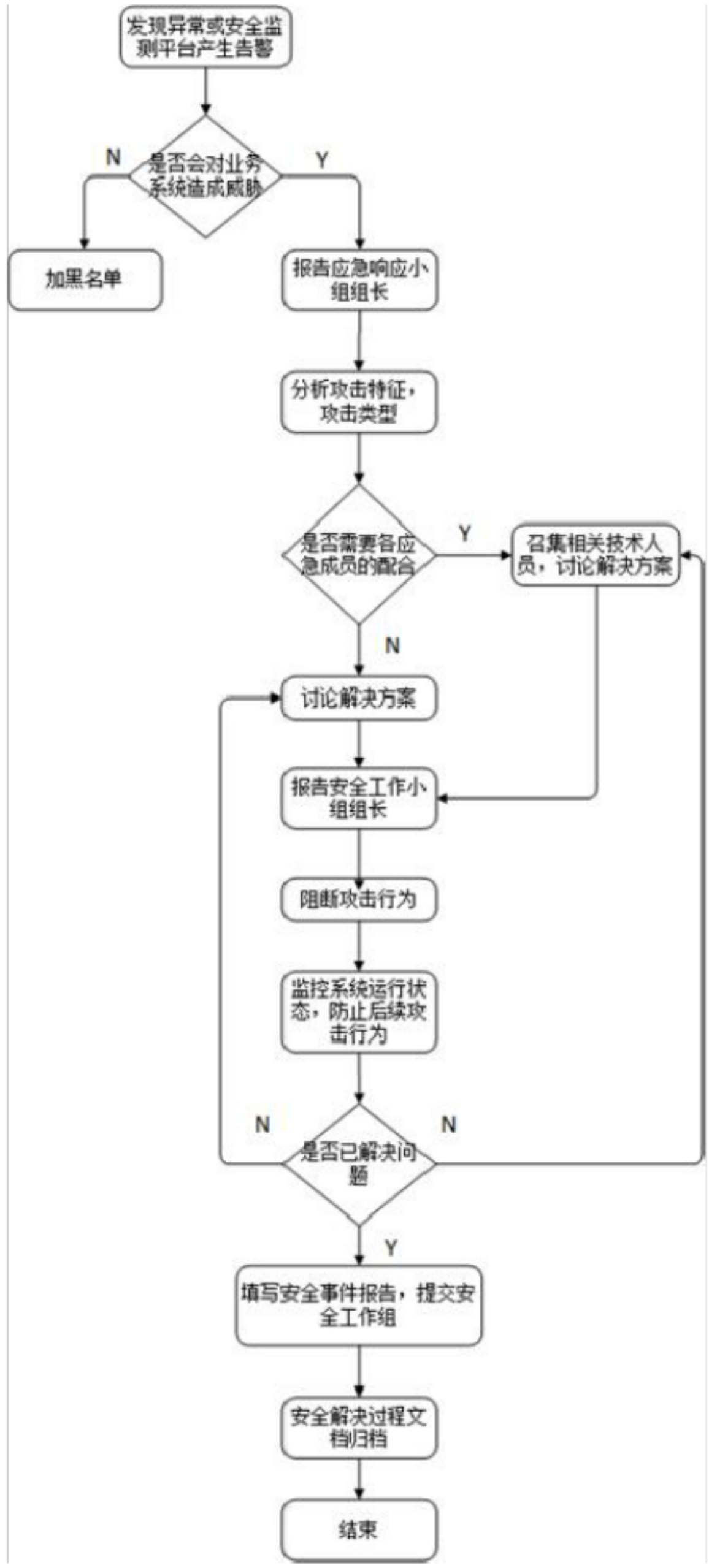
1.4 演练环境

本次演练完全模拟“护网行动”期间攻防演习环境，具体如下：

攻击方： 用手机开热点，使用互联网代理 IP，对 xx 系统进行攻击。

防守方：相关应急人员在攻防演习总指挥室。 监测攻击情况， 阻断攻击行为。

1.5 演练流程


发现异常或安全监测平台产生告警
是否会对业务系统造成威胁
N
Y
加黑名单
报告应急响应小组组长
分析攻击特征，攻击类型
是否需要各应急成员的配合
Y
召集相关技术人员，讨论解决方案
N
讨论解决方案
报告安全工作小组组长
阻断攻击行为
监控系统运行状态，防止后续攻击行为
N
是否已解决问题
N
Y
填写安全事件报告，提交安全工作组
安全解决过程文档归档
结束

2 演练方案

2.1 注意事项

1.攻击方向演练指挥报送演练　IP 地址。

2.演练过程中保留好入侵截图或相关证据；同时保留好相关阻断攻击行为的证据。

3.演练过程中有任何进展，攻防双方都向演练指挥汇报。

4.准备演练记录文档和表格。

2.2 演练场景

2.2.1 SQL注入漏洞

2.2.1.1 攻方渗透测试

风险名称	SQL 注入	风险级别	高
风险描述	攻击者可利用该漏洞，　获取网站管理账户密码等数据库敏感信息，　调用数据库函数执行系统命令，篡改、添加、删除网站数据和文件。		
测试过程	1) 利用工具探测漏洞地址、检测是否存在漏洞 2）查看当前数据库名称 3）查看当前数据库中的表		

2.2.1.2 防守方事件处理

序号	负责人员	操作事项
1	安全监控人员	监测平台查看到相关告警日志，根据攻击特征，判断该异常属于黑客 SQL注入行为，保留截图，上报技术研判小组负责人
2	技术研判小组组长、组员	分析测试页面是否存在　SQL注入漏洞，商讨处理方案。处理方案如下： 如果不存在此漏洞，网络管理员将　IP 拉入黑名单，如果存在　SQL漏洞，在将 IP 拉黑的同时，应用管理员修复此漏洞，对产生漏洞模块

		的参数进行有效性检测，对危险字符过滤，禁止 (' 、"、 +、 % &、 <>、 （）、 ; 、等) 特殊字符的传入。
3	技术研判小组组长	上报指挥部小组，提出解决方案，等待阻断下达命令
4	应急处置小组组长	网络管理员封禁 IP，应用管理员修复漏洞。与相关监测人员确定修复效果。
5	安全监控小组	继续监控系统状态，防止后续攻击行为
6	应急处置小组	填写安全事件处理报告，提交安全工作组。

2.2.2 Strust2 漏洞

2.2.2.1 攻方渗透测试

风险名称	Struts2 漏洞	风险级别	高
风险描述	攻击者利用此漏洞远程执行恶意代码， 如果 struts 框架为 root 或者 system 权限。 恶意用户可直接以系统最高权限控制服务器，威胁到内网安全。		
测试过程	1) 探测漏洞地址 2) 拿到 webshell 3）获取数据库权限		

2.2.2.2 防守方事件处理

序号	负责人员	操作事项
1	安全监控小组	监测平台查看到相关告警日志，根据攻击特征，判断该异常属于黑客利用 Struts2 漏洞进行攻击的行为，保留截图，上报技术研判小组负责人
2	技术研判小组组长、组员	分析测试页面是否存在 Struts2 漏洞，商讨处理方案。 处理方案如下：如果不存在此漏洞，网络管理员将 IP 拉入黑名单， 如果存在 Struts2 漏洞，在将 IP 拉黑的同时，应用管理员修复此漏洞，升级 struts2 框架。
3	技术研判小组组长	上报护网指挥组，提出解决方案，等待阻断下达命令
4	应急处置组	网络管理员封禁 IP，应用管理员修复漏洞。与相关监测人员确定修

		复效果。
5	安全监控人员	继续监控系统状态，防止后续攻击行为。
6	应急处置组	填写安全事件处理报告，提交安全工作组。

3 演练总结

演练总指挥：演练总指挥对演练进行总结，提出相关改进建议。

演练相关人员：演练相关人员对演练进行讨论，提出相关改进建议。

附 安全事件处理报告

安全事件处理报告

编写人： 编写日期：

攻击类型和特征	
应用系统名称	
事件描述	
应急处理时间	
事件上报过程	
应急处理过程	
事件处理结果上报	