网络安全实战攻防演练部署研究

张人杰[1],曾　振[2],肖　玮[3]

(1.湖南邮电职业技术学院,湖南长沙 410015;
2.湖南省通信产业服务有限公司,湖南长沙 410003;
3.湖南省教育厅,湖南长沙 410016)

【摘要】网络安全实战攻防演练是模拟真实网络环境对信息系统进行入侵攻击,发现潜在网络漏洞和安全隐患。通过对信息系统安全风险进行有效识别、分析和控制,从而提升网络安全意识和网络安全处置能力。文章结合网络安全攻防演练实际工作,对攻防演练战略部署、技术手段进行研究。

【关键词】网络安全;攻防演练;部署研究
【doi:10.3969/j.issn.2095-7661.2019.03.006】
【中图分类号】TP393.08　　【文献标识码】A　　【文章编号】2095-7661(2019)03-0023-03

Research on the deployment of offensive and defensive drill in network security actual combat

ZHANG Ren-jie[1], ZENG Zhen[2], XIAO Wei[3]

(1.Hunan Post and Telecommunication College, Changsha, Hunan, China 410015;
2.Hunan Communication Industry Service Co., Ltd., Changsha, Hunan, China 410003;
3. The Education Department of Hunan Province, Changsha, Hunan, China 410016)

Abstract: The network security combat of offensive and defensive drill is to simulate the real network environment to invade the information system and discover potential network vulnerabilities and security risks. Through the drill, the information system security risk is effectively identified, analyzed and controlled, so as to enhance the network security awareness and the ability of network security disposal. This paper studies the strategic deployment and technical means based on the actual work of network security combat of offensive and defensive drill.

Keywords: network security; offensive and defensive drills; deployment research

1 研究背景

为落实网络安全攻防演练要求,全力开展网络安全的整改和加固,提升网络安全水平,特开展网络安全攻防实战演练专项行动。[1]网络安全攻防演习是提升网络安全事件应急响应和处置能力的基础,是加强网络信息安全的有效手段,网络安全维系关键基础设施正常运转,特别涉及到通信保障、互联网生活等基础网络,属于重要资源。

通过网络安全攻防实战演练能够发现信息系统安全运维中存在的安全意识、技术措施和应急协调等方面的不足,树立安全防护意识,促进网络安全与应用安全的融合、促进网络安全运维部门与应用系统运维部门的合作,增强应急响应意识,进一步完善安全事件应急处置预案, 提升安全事件应急处置能力,以达到快速响应、准确定位、及时恢复的高效处置目标,有效提升网络安全保障能力[2]。

[收稿日期] 2019-06-30

[作者简介] 张人杰(1982-),男,汉族,湖南长沙人,湖南邮电职业技术学院副教授,网络工程师,硕士,研究方向:计算机网络技术、教育信息化。

[基金项目] 2018 年湖南邮电职业技术学院院级课题"'互联网 +'大数据背景下未来学习模式研究"(课题编号:18BZ05);2019 年湖南省教育科学"十三五"规划课题"教学诊改视域下数据挖掘在教育质量评价体系中的研究与实践"(课题编号:XJK19BZY029)。

2 组织架构部署

网络安全攻防演练工作要强化组织体系、值守监测、应急处置、信息报送、全网联动与改进提升。网络信息安全攻防演练组织架构见图 1。

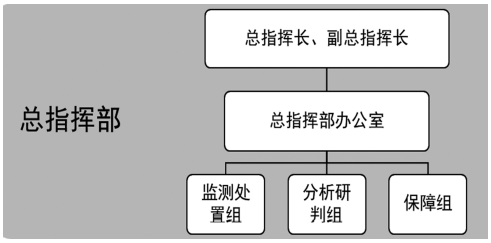

图 1 网络信息安全攻防演练组织架构图

2.1 成立总指挥部

演练总指挥部负责演习的领导、决策与指挥。总指挥部下设办公室,办公室负责落实总指挥长、副总指挥长的各项要求并向上汇报,对接外部单位,承接相关指令,对全网演习进行指挥,包括报送演习信息、进行威胁监测、情报共享、应急处置、分析研判与总结提升。

2.2 成立监测处置组

监测处置组负责利用技术手段监测重要网络与系统的威胁信息、接收汇总各单位上报的威胁信息,交付分析研判组进行研判;负责按分析研判组处置意见进行处置,并通过工单系统发全网进行处置;利用技术手段跟踪各单位处置完成情况。

2.3 成立分析研判组

分析研判组负责对总指挥办公室交付的需研判内容进行研判并及时回复研判结果,负责对监测处置组交付的威胁信息有效性、重要程度、后续处置措施等进行研判,及时将研判结果交付监测处置组。

2.4 成立保障组

保障组负责总指挥部运行保障等相关事宜,包括指挥部场地布置、办公条件、通信手段、专线、门禁、通讯录维护等。

3 技术部署

根据对各类信息系统安全风险评估,对以往网络安全事故分析,信息系统本身的脆弱性是安全风险的主要来源。系统脆弱性重点体现为:密码认证;弱口令;敏感数据泄露;SQL 语句注入;超权限控制[3]。

3.1 安全威胁级别

根据信息系统安全危害程度,安全威胁分为高级风险和中低级风险。

1)高级风险:高级风险可能直接导致系统被控制、核心数据泄露的风险。包括不局限于弱口令登录尝试、爆破登录尝试、SQL 注入尝试、任意文件上传漏洞利用尝试、任意文件下载漏洞利用尝试、心脏滴血漏洞利用尝试、远程代码 / 命令执行漏洞利用尝试、网页挂马尝试、后门利用尝试等。

2)中低级风险:中低级风险可能间接导致系统被控制、数据泄露的风险事件。包括不局限于 XSS 尝试、网站目录遍历漏洞利用尝试、网页失效的身份认证漏洞利用尝试等。

3.2 网络入侵技术

网络入侵通用手段为渗透技术。渗透技术主要以人工渗透为主,以攻击软件为辅,对存在安全弱点的目标网络和目标系统进行渗透入侵。渗透技术一般包含下列攻击工具:Acunetix Web Vulnerability Scanner 漏洞扫描工具、Metasploit Framework 缓冲区溢出测试工具、Shadow Security Scanner 安全漏洞扫描工具、Nmap 端口扫描器、ISS 漏洞扫描器、Firewalk 路由跟踪工具、Fragroute 网络入侵检测逃避工具等。另外还使用操作系统自带的一些网络命令工具,比如 Whois、Nslookup、Traceroute 等。除此之外,还包括如下一些网络入侵技术手段:

1)使用软件逆向技术检测各类信息系统的脆弱性,发现某些专用协议传输系统的逻辑问题,从而进行入侵;[4]

2)针对操作系统入侵,对操作系统组件服务进行二进制流量深度分析,从而获取系统用户相关敏感数据;

3)深度分析信息系统及网络拓扑结构和配置文件,抽丝剥茧,实现对站库分离目标的攻击;

4)混合利用漏洞,入侵信息系统,深透内网,把内网作为突破口进行入侵;

5)利用多漏洞互相配合,实现多网跨站攻击入侵;

6)利用已经发现的各类漏洞,比如“心脏滴血”漏洞进行入侵;

7)以物联网应用为入口,对门禁、监控、电子大屏、电子横幅、机顶盒等进行入侵,对点播链路进行定位分析,对网络系统管理员进行越权管理夺取;

8)从各类代码共享平台入手,找到敏感管理信息,掌握客户及员工信息,实现对信息系统全面控制;

9)社会工程学网络入侵,利用内网用户的好奇心、敏感心,从人入手,假冒各类名义发送钓鱼邮件、钓鱼短信,通过发表新媒体文章上传伪装成查杀工具的木马附件,通过现场、邮件、电话、微信、QQ 等套取敏感信息,进行社工入侵;

10)真实场景中的网络入侵,还包括 DDOS 和 CC 攻击。

3.3 应对措施

针对网络安全入侵各类技术手段,必须重点进行互联网暴露面清查、弱口令、源代码违规上传、工作

资料违规上传、信息系统预埋木马查杀、通过日志清查系统内信息是否已被黑客窃取等问题。对信息系统和电脑终端做到网络安全责任制。

1)进一步梳理网络与系统,清查僵尸系统,对于不必要的系统执行关停并断网。对无需开设公网访问的系统进行互联网暴露面清理。通过部署 IPS、WAF 对信息系统进行外网检测保护,通过部署堡垒机和动态感知系统对内网进行监控审计。

2)严格杜绝出现弱口令这一“零容忍”问题。在各层面严格执行账号数量最小化。口令设置建议要包含数字、大小写字母和特殊符号四类字符,长度不小于 8 位,并且不要出现数字连续、字母连续和键盘连续,口令也要避免包含用户名、姓名、生日、手机等个人信息。

3)网络层面上,严格落实端口开放最小化,仅开放必要的服务端口,除面向互联网用户开放的端口外,其他端口一律以最小化白名单形式做好访问控制。不仅包括对互联网开放的服务与端口,同样包括对内网开放的端口。

4)特别关注 21 端口和 3389 端口的清理,通过注册表和防火墙,对 3389 端口进行修改和屏蔽。

5)操作系统、数据库与 Web 应用层面上,做好漏洞补丁升级与安全基线配置,清理多余账号,严格控制账号操作权限,坚决杜绝出现弱口令。

6)在应用系统层面,清除不必要的子域名、网站上的外链。通过多种手段严防出现 SQL 注入、远程代码执行、远程命令执行漏洞。避免 WebShell 木马控制服务器,修改网页内容或添加黑页。

7)做好网络用户的社会工程学防范教育与普及,提高全员警惕,严防社工,不要点击不明邮件附件。提高安全意识,注意防范可疑人员通过现场、邮件、电话、微信、QQ 等套取敏感信息,交付敏感信息务必核实对方身份。

8)对各类信息系统和用户电脑终端严格执行“谁主管谁负责,谁使用谁负责”的原则,责任落实到人,签订网络信息安全承诺书。

4 总结与展望

网络安全实战攻防演练对信息系统安全风险进行有效识别、分析和控制,对提升网络安全意识和网络安全处置能力都有着十分重要的意义和实践价值。在进行网络安全实战攻防演练的同时,要避免断网、封 IP 等消极演练对抗方式。在演练要求上,要分层、分类、分级制定网络安全攻防标准,避免一刀切、一把尺解决网络安全问题。要充分调动各级单位的积极性,激发单位内生动力,针对性地选择关键、高价值的系统对象,从而引导网络安全攻防演练工作的良性互动和相向而行。

网络安全实战攻防演练在演练方法上从背靠背转向面对面形式,模式上从比赛形式转向研究形式,考核方式上多样化,演练时间上常态化。对出现的网络安全问题,不能只靠曝光、张榜来解决,要刚柔相济,重点帮扶。对各级单位开展个性化评估和柔性化支撑,从而促进网络信息安全产业的良性发展[5]。

【参考文献】

[1]王钧玉.基于攻击事件的动态网络风险评估框架研究[J].湖南邮电职业技术学院学报,2018(3):41-43.

[2]刘阳.网络安全攻防演练的部署与方案设计[J].网络空间安全,2017(11):15-16.

[3]杨名.高校无线数字化校园网络安全防护方案研究[J].轻工科技,2019(8):104-105.

[4]郝叶力.网络安全攻防演练的亮点、痛点和要点[J].信息安全研究,2018(5):30-32.

[5]王春梅.当前政务网络信息面临的安全威胁及其防护策略[J].电子世界,2014(16):12-13.

(上接第 22 页)

[6]李辉,张安,赵敏.粒子群优化算法在 Fir 数字滤波器设计中的应用[J].电子学报,2005(7):1338-1341.

[7]董龙昌,陈民铀,李哲.基于 V2G 的电动汽车有序充放电控制策略[J].重庆大学学报,2019(1):1-15.

[8]樊华羽,詹浩,程诗信.基于 α-stable 分布的多目标粒子群算法研究及应用[J].西北工业大学学报,2019(2):232-241.

[9]吴俊俊,宋刚,卢彬芳.基于粒子群优化算法的特高压输电线路覆冰不平衡张力计算[J].浙江电力,2019(3):59-64.