渗透测试在网络安全等级保护测评中的应用

王世轶 吴 江 张 辉
(上海市网络技术综合应用研究所 上海 200233)

摘 要 渗透测试能真实地评估信息系统抵御网络入侵的能力,成为信息系统安全评估的一个有效手段。介绍渗透测试在网络安全等级保护测评中的必要性和重要性;详细描述渗透测试的原理、流程、使用的工具、风险规避方法等。通过案例介绍渗透测试在网络安全等级保护测评中实施过程及风险应对措施,并对存在的问题提出整改建议,为信息系统后续安全防护措施提供指导。

关键词 网络安全 等级保护 渗透测试

中图分类号 TP3 **文献标识码** A DOI:10.3969/j.issn.1000-386x.2018.11.032

THE APPLICATION OF PENETRATION TEST IN THE EVALUATION OF NETWORK SECURITY CLASSIFIED PROTECTION

Wang Shiyi Wu Jiang Zhang Hui
(*Shanghai Institute for Integrated Application of Network Technology*, *Shanghai 200233*, *China*)

Abstract Penetration testing can truly evaluate the ability of information system in resisting network intrusion, which becomes an effective means of information system security assessment. We introduced the necessity and importance of penetration test in the evaluation of network security classified protection, and described the principle, process, tools, and risk aversion method of the penetration test in detail. We also introduced the implementation process and risk response measures of penetration testing in network security classified protection evaluation through a case. Suggestions were put forward on the existing problems. It provides guidance for subsequent security protection measures of information system.

Keywords Network security Classified protection Penetration testing

0 引 言

网络安全等级保护制度是落实国家网络安全法要求的重要措施之一。伴随着信息技术的飞速发展,新的安全漏洞层出不穷,导致信息系统存在的安全隐患越来越多。因此,在等级保护测评过程中如何及时、准确地发现系统存在的安全风险,成为非常迫切的需求。渗透测试模拟攻击者的思维,采用手动或技术成熟的工具对被测系统的安全性进行全面评估,从而最大程度地发现系统存在的安全隐患,成为等级保护测评中一个必不可少的重要环节。

1 渗透测试概述

1.1 渗透测试在等保测评中的必要性

2017 年 6 月 1 日,《中华人民共和国网络安全法》正式实施,明确要求国内运营的信息系统须实施等级保护制度,使等级保护制度成为国家基本制度并上升到法律层面。在等级保护的基本要求中,虽没有相应的技术标准对信息系统“抗渗透”能力做明确规定,但针对定级为第三级及以上的信息系统,在基本要求的安全技术层面,对系统抵御大规模恶意攻击能力、非法入侵检测与防御能力、抗恶意代码攻击能力、安全事件

收稿日期:2018-04-25。**王世轶**,工程师,主研领域:等级保护测评,信息安全。**吴江**,工程师。**张辉**,学士。

应急响应及监控等能力做了详细要求。同时在安全管理层面,要求信息系统须经过公正的第三方安全测试才能上线运行。

鉴于上述条件约束,被测信息系统若未进行渗透测试,则无法满足等级保护相关要求。渗透测试在等保测评中的实施,一方面检查并验证被测信息系统存在的安全漏洞,提供切实可行的修复建议;另一方面,有助于等级保护测评质量的提升。

1.2　渗透测试原理

渗透测试主要依据业界公布的或测试人员掌握的安全漏洞信息,采用攻击者的思维方式,通过工具或手工方式对目标的应用、主机、网络、数据库等安全性进行深入探测,发现系统最脆弱的环节的过程。渗透测试一个重要的原则,即所有的测试行为必须在用户的书面明确授权和监督下进行,经授权的渗透测试,目的是真实、全面地发现信息系统存在的脆弱性并验证其可用,不再进行后续渗透操作(如植入后门等),因此,一般不会对信息系统造成危害和损失。

1.3　渗透测试流程

通常,渗透测试一般包括测试准备、信息探测、测试实施、报告编制四个阶段,具体流程如图 1 所示。

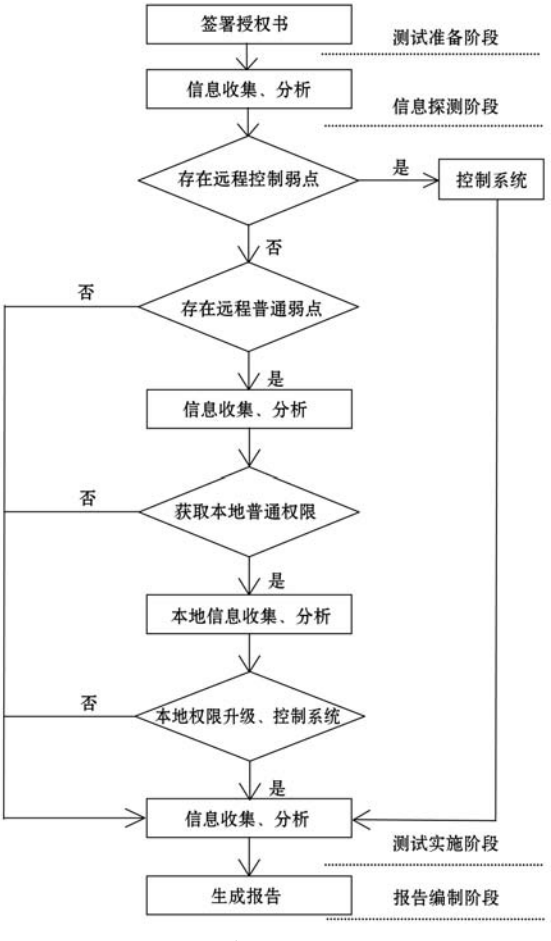

图 1　渗透测试流程图

各个环节相关工作内容概述如下:

(1) 测试准备阶段　在获取到单位的书面授权许可后,开始渗透测试的实施。将实施范围、方法、工具、时间、人员等具体方案与单位进行交流,沟通可能存在的测试风险,并得到单位的认可。整个测试过程都在单位的监督和控制下进行。

(2) 信息探测阶段　渗透测试过程中,根据规定的测试范围收集信息系统相关信息,可采用一些商业或开源的安全评估工具进行收集,如 Webinspect、Appscan、Nessus、Nmap 等,并对探测到的端口、服务、IP、DNS、OS 等信息进行整理,为下一步测试实施阶段提供支撑。

(3) 测试实施阶段　渗透测试人员对探测到的信息进行分析,通过制定渗透策略、准备攻击代码、研究绕过机制等步骤进行测试。实施路径主要包括内网和外网两种:

① 内网测试　从内网发起对信息系统的测试工作,目的是避开防火墙等设备的安全防护措施。此阶段如能成功,可能获得普通用户权限,然后通过提权等操作,获取系统的最高权限。以被控制的服务器作为跳板,从而对其他目标进一步渗透测试。

② 外网测试　直接通过互联网,对信息系统进行渗透测试,操作流程与内网测试类似。

(4) 报告编制阶段　实施人员分析测试结果,编写系统渗透测试报告,主要包括具体测试结果、漏洞结果评估及整改建议等内容。

1.4　渗透测试的风险规避

渗透测试是动态变化的,测试过程仍可能对应用、主机、网络等正常运行带来一定的影响。为了最大程度上避免测试过程对业务运行造成影响,需要实施风险规避的策略,具体如下:

(1) 方案评审　双方签署渗透测试委托书,制定并评审渗透测试方案,得到双方的认可。

(2) 时间策略　选择合适的测试时间,如选择夜间或业务量不高的时间段进行测试,最大程度上避免测试过程对业务造成影响,同时预留风险排除时间。

(3) 攻击策略选择　对于实时性要求高的核心业务系统,不建议做深入测试,如 DDOS 类测试,测试人员可对结果做分析推测,而不验证危险的操作。

(4) 系统备份和恢复　在测试实施前,需对被测系统做完整备份,当出现问题时可及时恢复,针对核心业务系统建议对备份系统进行渗透测试。

(5) 应急策略 当被测系统出现中断、响应缓慢等问题时,需及时停止测试工作,配合被测单位进行故障处置,在故障处理完毕后,经单位授权才能继续进行剩余的测试。

(6) 沟通策略 双方建立干系人联络表,确定接口人,对测试过程中出现的问题及时沟通,并确保沟通有效。

1.5 渗透测试工具介绍

在渗透测试过程中,测试人员使用操作系统自带网络应用、诊断工具或开源及商业软件,以及自行开发的安全扫描工具。这些工具在技术上已经非常成熟,具有高度安全和可控性,并能根据测试者的实际要求进行有针对性的测试。但安全工具本身也是一把双刃剑,需针对系统可能出现的问题提出相应对策,以确保在渗透测试的过程中保持在可控状态。

(1) 系统自有工具 表 1 列出了常用的系统自带网络应用、管理和诊断工具,测试人员将用到但不限于以下命令进行测试。

表 1 系统自有工具表

工具名称	获取途径	主要用途	风险等级
ping	系统自带	获取主机信息	无
telnet	系统自带	登录系统	无
ftp	系统自带	传输文件	无
tracert	系统自带	获取网络信息	无
net use	系统自带	建立连接	无
net user	系统自带	查看系统用户	无
echo	系统自带	文件输出	无
nslookup	系统自带	获取主机信息	无

(2) 其他测试工具 表 2 列出了渗透测试中常用到的网络扫描工具、网络管理软件等,测试人员将可能用到但不限于以下工具。

表 2 其他测试工具表

工具名称	获取途径	主要用途	风险等级	风险控制方法
nmap	互联网	获取主机开放的服务、端口信息	无	无
Nessus	互联网	对主机进行漏洞扫描	可能造成网络资源占用	如果主机负载过高,停止扫描
nc	互联网	端口连接工具	无	无
Burpsuit	互联网	通过漏洞本地提升权限	溢出程序可能造成服务不稳定	备份数据,服务异常时重启服务

2 渗透测试实施

本文通过一个实例来说明渗透测试是如何在等保测评中实施的。在某单位等保三级系统测评中,需对用户的 WEB 系统进行渗透测试,以验证信息系统的整体安全防护水平。

2.1 方案制定

渗透测试小组根据信息系统的规模和实际业务情况制定详细的渗透测试方案,包括制定合理的渗透测试计划、选择适当的测试方法、充分准备测试工具,分析测试过程中可能带来的风险和相应的风险规避方法等。

2.2 信息收集

渗透测试人员使用多种系统或工具进行信息收集工作,包括系统扫描工具 Nmap、Openvas、Burpsuit 等,经扫描发现系统开放了 80、139、445、3389、47001 等端口。针对这些服务从系统层面和 WEB 层面进行分析,发现系统存在文件共享、远程接入、SQL 注入、XML 注入等漏洞,为下一步的漏洞利用提供基础。

另外,针对信息收集阶段的测试方法、测试内容及可能存在的风险,做了应急处置策略,具体如表 3 所示。

表 3 信息收集风险控制表

测试方法	测试内容	风险等级	存在风险	风险控制方法
扫描	获取系统主机、应用程序和数据库的相关信息,并对扫描结果进行分析。	低	扫描,可能消耗服务器一定性能	终止扫描

2.3 测试实施

根据获取的漏洞信息,结合信息系统的特点、异构性等方面对漏洞进行确认,并制定渗透测试策略。获取的信息发现高危漏洞,尝试直接利用高危漏洞,验证是否可用。下面以“文件共享”漏洞为例,介绍测试过程。

第一步　制定渗透测试策略:1）目标:获取被测系统服务器的控制权限;2）实施途径:系统漏洞扫描 --> 服务漏洞 --> 漏洞利用 --> 获取远程 Shell --> 建立用户 --> 远程桌面;3）说明:如果获取的远程 Shell 权限较低,则需提权后再建立用户。

第二步　采用不同的漏扫工具对已扫描的漏洞进行确认,结果确认系统服务器存在熟知漏洞(扫描工具为 nmap 和 Nessus),编号为 MS08 - 067。该漏洞是针对文件共享服务的,若服务器收到特制的 RPC 请求,则该漏洞可能允许远程执行代码。

第三步　漏洞确认之后,采用漏洞利用工具实施溢出,顺利获取 Shell 控制界面,执行“whoami”命令,查看“用户及用户组”,显示为“Administrator”用户组,表明获取的是系统管理员的权限,即获取系统最高控制权。

第四步　通过该 Shell 建立后门帐号,后续使用后门帐号即可远程登录系统,至此整个过程完成(该步骤获得用户许可)。

另外,在测试实施阶段,测试人员通过前期收集到的信息,对单位被测信息系统进行工具或手工测试。针对测试对象和测试方法以及可能出现的风险做了应急处置策略,具体如表 4 所示。

表 4　测试实施风险控制表

测试对象	测试内容	风险等级	存在风险	风险控制方法
WEB 系统	SQL 注入	高	检测过程不影响业务	无
	跨站脚本(XSS)	高	检测过程不影响业务	无
	跨站请求伪造(CSRF)	中	检测过程不影响业务	无
	文件上传漏洞	高	检测过程不影响业务	无
	目录遍历漏洞	中	检测过程不影响业务	无
	数据库泄露	高	检测过程不影响业务	无
	越权访问	高	检测过程不影响业务	无
	会话验证绕过	中	检测过程不影响业务	无
	中间件漏洞	高	检测过程不影响业务	无
	加密传输	高	检测过程不影响业务	无
	敏感信息泄露	高	检测过程不影响业务	无
	恶意代码	中	检测过程不影响业务	无
	口令破解	中	可能会影响网络性能	停止破解
	嗅探(内网)	中	可能出现短暂断网现象	停止嗅探
	缓冲区溢出	高	可能出现未知错误	停止测试

2.4　报告输出

渗透测试完成后,测试人员整理工作内容和成果。根据发现的安全漏洞和安全风险提出系统存在的问题,并有针对性的提出问题整改建议,形成《渗透测试报告》。

3　结　语

本次对该单位 WEB 系统进行的渗透测试,模拟黑客成功获取服务器的最高控制权限,并获取后台数据库数据信息。系统层面的漏洞主要是由于软件开发过程中的缺陷,一般需要严密跟踪软件厂商的安全预警,及时更新系统补丁。因此,建议用户构建漏洞预警与更新机制,在日常的安全维护中,对重要系统定期进行漏洞扫描,并在确认安全的基础上更新补丁。在等级保护项目中实施渗透测试,能及时发现信息系统存在的安全风险,做好预防措施,也能更好地满足等级保护相关要求,保障被测信息系统安全、稳定运行。

参　考　文　献

[1] 常艳,王冠. 网络安全渗透测试研究[J]. 信息网络安全,2012(11):3 - 4.

[2] 毛忠亮. 基于图的渗透测试方法的研究[D]. 长春:长春工业大学,2016.

[3] 孙艳,宋巍. 等级保护测评中邮件系统应用安全测评方法的研究[C]//全国信息安全等级保护技术大会会议. 2013.

[4] 王绍强,邵丹,王艳柏. 网络渗透测试技术分析研究[J]. 电子世界,2015(17):154 - 155.

[5] 蒲福连. 基于协同自主的网络渗透测试技术研究[D]. 成都:电子科技大学,2014.

[6] 林开彬,宋瑜琦,毛锡军. 基于 Kali Linux 的渗透测试方法探析[J]. 福建电脑,2017,33(10):11 - 12.

[7] 张明舵,张卷美. 渗透测试之信息搜集的研究与漏洞防范[J]. 信息安全研究,2016,2(3):211 - 219.

[8] 杨理文. 基于渗透测试的网络安全评估技术研究[D]. 长沙:国防科学技术大学,2011.