校园网渗透测试

（2021-2022 学年）

策

划

书

日期：二〇二二年十月四日

目录

一、 引言

伴随着学校业务的发展，河南理工大学的网站、系统等都进行了不同程度的功能更新和系统投产，同时，系统安全要求越来越高，可能受到的恶意攻击包括:信息篡改与重放、信息销毁、信息欺诈与抵赖、非授权访问、网络间谍、“黑客”入侵、病毒传播、特洛伊木马、蠕虫程序、逻辑炸弹、APT 攻击等。 这些攻击完全能造成信息系统瘫痪、重要信息流失。

二、 测试概述

2.1. 测试简介

本次测试内容为渗透测试

渗透测试：渗透测试是通过模拟恶意黑客的攻击方法，来评估计算机网络系统安全的一种评估方法。

2.2. 测试依据

※GB/T 18336-2001《信息技术 安全技术信息技术安全性评估准则》

※GB/T 20274-2006《信息系统安全保障评估框架》

2.3. 测试思路

（1）信息收集

通常被称作“踩点”，是进行攻击入侵的首要任务。收集信息系统的网络信息，主要是为了制定有目的性和针对性的渗透测试计划和方案，来减小被发现的概率、提高测试的成功率、减小漏报率。“踩点”的主要内容有扫描主机域名和 IP 地址、判断操作系统类

型、发现系统开放的端口及该端口对应的应用程序、扫描系统账号列表、收集系统配置信息等。信息收集常用的工具有 BT5、nmap、X-Scan、Appscan 等。

（2）端口扫描

端口扫描是通过扫描目标地址的开放端口，发现其所开放的所有服务来确定系统的基本特征，这是进行渗透测试的基础步骤，安全测试者通过扫描结果并结合经验发现系统可被利用的安全缺陷，为进一步的渗透提供依据。

（3）远程溢出

远程溢出攻击是通过远程终端对信息系统实现溢出攻击的方式，它由于较易掌握和实施，导致成为出现频率最高、威胁最严重的渗透测试方式，通常只要攻击者具备基础网络常识就能通过利用现成的远程溢出攻击工具实现这种攻击。

（4）本地溢出

本地溢出是指本地计算机因程序数据溢出而关闭或无法执行。本地溢出攻击是指在本地执行一段特定的代码指令导致本地计算机程序溢出从而获得管理员权限的方法，使用该攻击方法的前提是需要经过口令猜测或暴力破解获得普通用户的密码口令。由于本地计算机设置了弱口令的不当密码策略导致了本地溢出，在使用普通用

户登录到系统后对未部署主动安全防御的系统实施本地溢出攻击，达到获得完全控制管理权限的目的。

（5）网络嗅探

嗅探是进行信息收集的一种方法，主要是用来捕捉网络中像明文密码这样的传输数据的方法，同时也能够抓取特定计算机之间的完整会话信息。要强调的是为了达到捕获网络中所有传输数据的目的，通常要求计算机的网卡模式在嗅探时设置为混合模式，嗅探器或计算机需要直连到网络来获取大量数据信息，所以嗅探常被用在内部测试。

（6）SQL 注入攻击

SQL 注入是指在网站中的 Web 表单、字符查询输入框中，通过提交某些特殊 SQL 语句达到篡改网站后端采用数据库中内容的方式。SQL 注入攻击是黑客攻击数据库的常用技术手段之一，由于网站没有详细的过滤用户输入的数据导致存在 SQL 注入漏洞，这也是非法数据侵入数据库系统的主要原因。

（7）跨站脚本攻击

跨站脚本攻击是指攻击者将具有恶意目的的数据潜入到远程用户信任的 WEB 页面的 HTML 代码中，当该页面被浏览器下载运行时嵌入的脚本将被执行，用户页面被跳转到攻击者精心编织的其他页

面，用户毫无顾及的填写各种敏感信息，殊不知已被攻击者盗取或被站点挂马控制。

（8）暴力破解

暴力攻击的主要目的是通过尝试各种密码字典和穷举法查出合法的用户名和口令，所采用的字典比较庞大，比如最常使用的彩虹表有 100G 以上，这种字典由大量的字母、数字、符号等组合而成的，虽比较完善但这种破解用户口令的方法是很耗时的，并且可能会造成系统过载而无法响应合法的请求。另外若系统开启了帐户锁定策略，这种口令尝试攻击会关闭合法登录帐户。

（9）漏洞扫描

漏洞扫描是针对目标系统的穷举检查发现系统是否存在漏洞的一种方法。扫描的目标范围包括网络设备、主机操作系统、数据库管理系统及应用系统，它通常是使用自动化工具执行的，如绿盟漏洞扫描设备，这些工具能够测试目标范围内已知漏洞方面的大量潜在弱点，并出具漏洞扫描报告，罗列系统潜在的安全问题并提供整改方案。

（10）代码审查

代码审查主要是通过手工或审查工具对被测业务信息系统进行安全代码审查，发现可能会导致安全问题的不安全编码规范、编码

技术和代码漏洞。代码审查测试工作包括：审查代码中的 XSS 脚本漏洞；审查代码中的 SQL 注入漏洞；审查代码中的缓冲区溢出漏洞；审查不规范的编码技术；另外也包括发现软件代码编写错误及其他潜在漏洞的审查。

三、 渗透测试的风险规避

在渗透测试的过程中，我们会尽量避免做影响正常业务运行的操作，也会试试风险规避的计策。并且不会影响学校网站数据，采取一下多条策略来规避渗透测试带来的风险。

时间策略：

为减轻渗透测试造成的压力和预备风险排除时间，一般的安排测试时间在学校业务不高的时间段。

测试策略：

为了防范测试导致业务的终端，可以不做一些拒绝服务类的测试。非常重要的系统不做深入的测试，避免意外崩溃而造成不可挽回的损失；具体测试过程中，最终结果可以由测试人员做推测，而不实施危险的操作步骤加以验证等。

备份策略：

为防范渗透过程中的异常问题，测试的目标系统需要事先做一个完整的数据备份，以便在问题发生后能及时恢复工作。对于核心业务系统等不可接受可能风险的系统的测试，可以采取对目标副本进行渗透的方式加以实施。这样就需要完整的复制目标系统的环境:

硬件平台、操作系统、应用服务、程序软件、业务访问德国；然后对该副本再进行渗透测试；

应急策略:

测试过程中，如果目标系统出现无响应、中断或者崩溃等情况，我们会立即中止渗透测试，并配合业主单位技术人员进行修复处理等。在确认问题、 修复系统、防范此故障再重演后，经业主单位方同意才能继续进行其余的测试。

四、渗透测试工具介绍

渗透测试人员模拟黑客入侵攻击的过程中使用的是操作系统自带网络应用、管理和诊断工具、黑客可以在网络上免费下载的扫描器、远程入侵代码和本地提升权限代码以及某某自主开发的安全扫描工具。这些工具经过全球数以万计的程序员、网络管理员、安全专家以及黑客的测试和实际应用，在技术上已经非常成熟，实现了网络检查和安全测试的高度可控性，能够根据使用者的实际要求进行有针对性的测试。但是安全工具本身也是一把双刃剑， 为了做到万无一失，们也将针对系统可能出现的不稳定现象提出相应对策,以确保服务器和网络设备在进行渗透测试的过程中保持在可信状态。

五、渗透结束

1. 提供系统性能优化改进方案。
2. 提供漏洞修复报告。
3. 测试过程中、测试后提出改进意见，测试后配合做好系统优化改进工作，提供回归测试。