XXX 渗透测试方案

■ 文档编号

■ 密级

■ 版本编号

■ 日期

!

■ 版本变更记录

时间	版本	说明	修改人

■ 适用性声明

本文档是〔以下简称“某某”〕为 XXX〔以下简称“XXX”〕提交的渗透测试方案，供 XXX 的工程相关人员阅读。

名目

一. 概述

1.1 工程背景

XXX 成立于 1992 年，注册资金 7 亿元，具有中国房地产开发企业一级资质,总资产300多亿元，是一个涵盖房地产开发、商业治理、物业治理、商贸代理、综合投资业务的大型集团企业。

多年来,XXX 信息系统的进展与信息化的建设密不行分，并且通过领导重视、业务需求、自身努力已经将信息化程度提高到肯定的水平.但近年来针对 XXX 信息系统的安全大事时有发生，网络面临的安全威逼日益严峻。随着业务需求不断地增加、网络构造日趋简单，信息系统面临的安全威逼、威逼的主体及其动机和力量、威逼的客体等方面都变得更加简单和难于掌握。

XXX 信息系统的建设是由业务系统的驱动建设而成的,初始的网络建设大多没有统一的安全规划，而业务系统的业务特性、安全需求和等级、使用的对象、面对的威逼和风险各不相同.在支持业务不断进展的前提下，如何保证系统的安全性是一个巨大的挑战，对系统进展区域划分，进展层次化、有重点的保护是保证系统和信息安全的有效手段，信息安全体系化的建设与开展迫在眉睫。

1.2 实施目的

信息安全越来越成为保障企业网络的稳定运行的重要元素。XXX 信息系统经过多年的实践和摸索，已经初具规模，在技术上、产品方面取得了很大的成就，但随着企业面临的安全威逼不断变化，单纯地靠产品来解决各类信息安全问题已经不能满足XXX 的实际安全需求。从根本上解决目前企业所面临的信息安全难题,只靠技术和产品是不够的，效劳将直接影响到解决各类安全问题的效果.

对于已经实施了安全防护措施〔安全产品、安全效劳〕或者马上实施安全防护措施的 XXX 而言，明确

网络当前的安全现状对下一步的安全建设具有重大的指导意义。所以本次工程的目的是通过远程渗透测试全面检测XXX 信息系统目前存在安全隐患，为下一步信息安全建设供给依据.

我们信任，凭借某某多年的安全技术积存和丰富的安全效劳工程阅历,能够圆满的完本钱次安全效劳工程.同时，我们也期望能连续保持和 XXX 在信息安全工程上长期的合作，共同为XXX 信息系统的安全建设奉献力气。

1.1 效劳目标

某某在本次XXX 信息安全效劳工程中将到达以下的目标:

通过远程渗透测试全面检测XXX 信息系统直接暴露在互联网上的安全隐患，并供给实际可行的安全修复建议。

二. 远程渗透测试介绍

2.1 渗透测试原理

渗透测试过程主要依据某某安全专家已经把握的安全漏洞信息,模拟黑客的真实攻击方法对系统和网络进展非破坏性质的攻击性测试。这里，全部的渗透测试行为将在客户的书面明确授权和监视下进展。

2.2 渗透测试流程

方案制定

某某猎取到 xxx 的书面授权许可后，才进展渗透测试的实施.并且将实施范围、方法、时间、人员等具体的方案与xxx 进展沟通，并得到xxx 的认同。

在测试实施之前，某某会做到让 xxx 对渗透测试过程和风险的知晓，使随后的正式测试流程都在xxx 的掌握下。

信息收集

这包括:操作系统类型指纹收集；网络拓扑构造分析；端口扫描和目标系统供给的效劳识别等。可以承受一些商业安全评估系统(如：ISS、极光等〕；免费的检测工具〔NESSUS、Nmap 等)进展收集。

测试实施

在躲避防火墙、入侵检测、防毒软件等安全产品监控的条件下进展：操作系统可检测到的漏洞测试、应用系统检测到的漏洞测试〔如：Web 应用〕，此阶段假设成功的话，可能获得一般权限。

渗透测试人员可能用到的测试手段有：扫描分析、溢出测试、口令爆破、社会工程学、客户端攻击、中间人攻击等，用于测试人员顺当完成工程。在猎取到一般权限后，尝试由普

通权限提升为治理员权限，获得对系统的完全掌握权。一旦成功掌握一台或多台效劳器后，测试人员将利用这些被掌握的效劳器作为跳板，绕过防火墙或其他安全设备的防护，从而对内网其他效劳器和客户端进展进一步的渗透。此过程将循环进展,直到测试完成.最终由渗透测试人员去除中间数据。

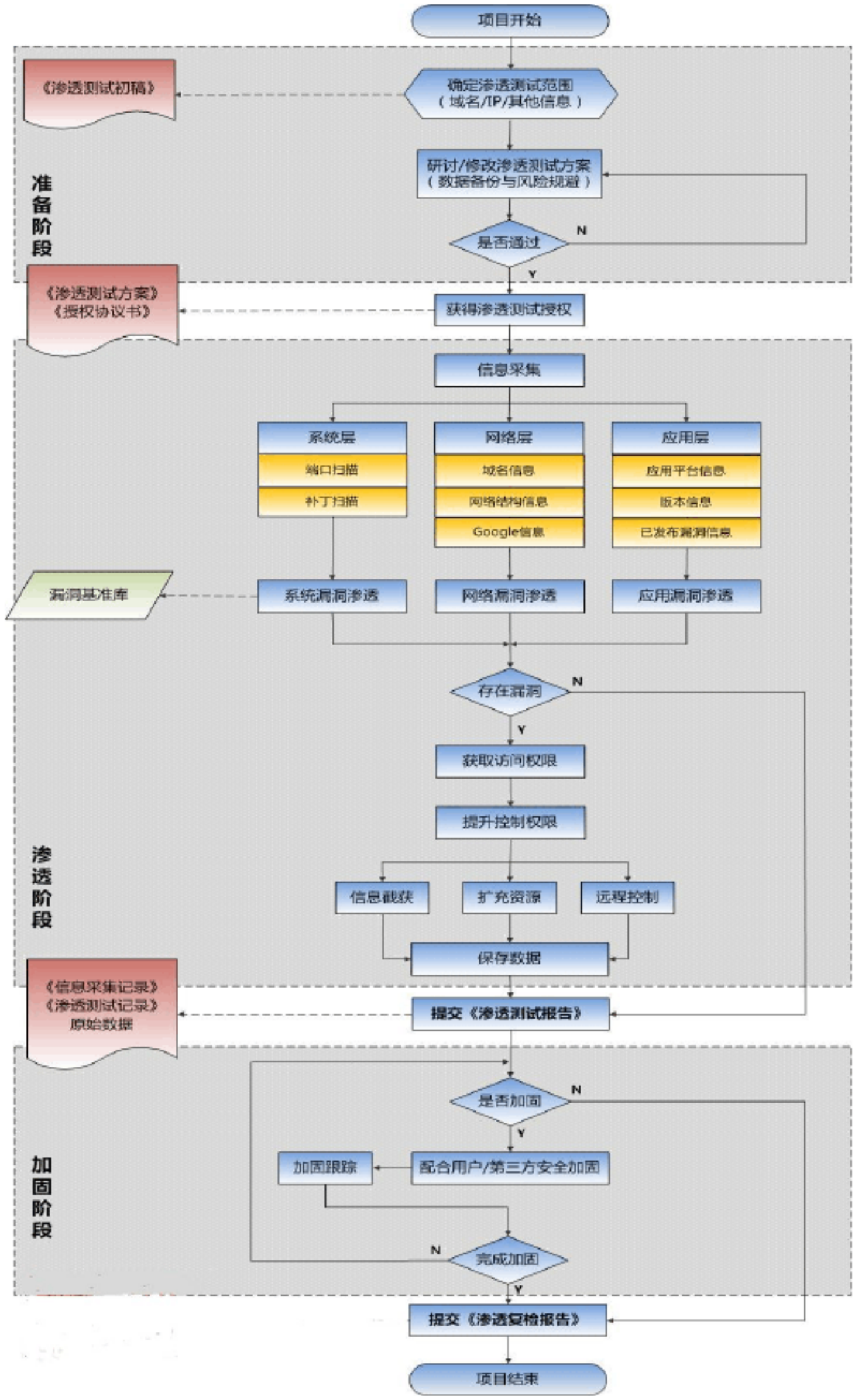
报告输出

渗透测试人员依据测试的过程结果编写直观的渗透测试效劳报告。内容包括：具体的操作步骤描述；响应分析以及最终的安全修复建议。

安全复查

渗透测试完成后，某某帮助 XXX 对已觉察的安全隐患进展修复.修复完成后，某某渗透测试工程师对修复的成果再次进展远程测试复查，对修复的结果进展检验,确保修复结果的有效性。

以下图是更为具体的步骤拆分示意图：


项目开始
《渗透测试初稿》
确定渗透测试范围
（域名/IP/其他信息）
研讨/修改渗透测试方案
（数据备份与风险规避）
是否通过
N
Y
准备阶段
《渗透测试方案》
《授权协议书》
获得渗透测试授权
信息采集
系统层
端口扫描
补丁扫描
网络层
域名信息
网络结构信息
Google信息
应用层
应用平台信息
版本信息
已发布漏洞信息
漏洞基准库
系统漏洞渗透
网络漏洞渗透
应用漏洞渗透
存在漏洞
N
Y
获取访问权限
提升控制权限
信息截获
扩充资源
远程控制
保存数据
渗透阶段
《信息采集记录》
《渗透测试记录》
原始数据
提交《渗透测试报告》
是否加固
N
Y
加固跟踪
配合用户/第三方安全加固
完成加固
N
Y
加固阶段
提交《渗透复检报告》
项目结束

某某渗透测试流程图