网络安全测评技术与标准

网络安全测评概况
网络安全测评类型
网络安全测评流程与内容
网络安全测评技术与工具
网络安全测评质量管理与标准

文老师软考教育

网络安全测评概况

文老师软考教育

◆网络安全测评概念：网络安全测评是指参照一定的标准规范要求，通过一系列的技术和管理方法，获取评估对象的网络安全状况信息，对其给出相应的网络安全情况综合判定。网络安全测评对象通常包括信息系统的组成要素或信息系统自身，如表所示。

测评对象	测评内容概况
信息技术产品安全测评	对信息技术相关产品（包括信息安全产品）的安全性进行测试和评估，相关产品主要有操作系统、数据库、交换机、路由器、应用软件等。信息安全产品主要有防火墙、入侵检测、安全审计、VPN、网络隔离、安全操作系统、安全数据库系统、安全路由器、UTM等。按照测评依据和测评内容，测评常见类型包括信息安全产品分级评估、信息安全产品认定测评、信息技术产品自主原创测评、源代码安全风险评估、选型测试、定制测试
信息系统安全测评	对信息系统的安全性进行测试、评估、认定。按照测评依据和测评内容，主要包括信息系统安全风险评估、信息系统安全等级保护测评、信息系统安全验收测评、信息系统安全渗透测试、信息系统安全保障能力评估等

网络安全测评类型

◆基于测评目标分类：按照测评的目标，网络安全测评可分为：

1．网络信息系统安全等级测评。是测评机构依据国家网络安全等级保护相关法律法规，按照有关管理规范和技术标准，对非涉及国家秘密的网络信息系统的安全等级保护状况进行检测评估的活动。主要检测和评估信息系统在安全技术、安全管理等方面是否符合已确定的安全等级的要求；对于尚未符合要求的信息系统，分析和评估其潜在威胁、薄弱环节以及现有安全防护措施，综合考虑信息系统的重要性和面临的安全威胁等因素，提出相应的整改建议，并在系统整改后进行复测确认，以确保网络信息系统的安全保护措施符合相应安全等级的基本安全要求。目前，采用网络安全等级保护2.0标准。

2．网络信息系统安全验收测评。是依据相关政策文件要求，遵循公开、公平和公正原则，根据用户申请的项目验收目标和验收范围，结合项目安全建设方案的实现目标和考核指标，对项目实施状况进行安全测试和评估，评价该项目是否满足安全验收要求中的各项安全技术指标和安全考核目标，为系统整体验收和下一步的安全规划提供参考依据。

3．网络信息系统安全风险测评。是从风险管理角度，评估系统面临的威胁以及脆弱性导致安全事件的可能性，并结合安全事件所涉及的资产价值来判断安全事件一旦发生对系统造成的影响，提出有针对性的抵御威胁的方法措施，将风险控制在可接受的范围内，达到系统稳定运行的目的，为保证信息系统的安全建设、稳定运行提供技术参考。从技术和管理两方面进行，包括系统调查、资产分析、威胁分析、技术及管理脆弱性分析、安全功能测试、风险分析等，出具风险评估报告，提出安全建议。

网络安全测评类型

文老师软考教育

◆基于测评内容分类：依据网络信息系统构成的要素，网络安全测评可分成两大类型：技术安全测评和管理安全测评。其中，技术安全测评主要包括物理环境、网络通信、操作系统、数据库系统、应用系统、数据及存储系统等相关技术方面的安全性测试和评估。管理安全测评主要包括管理机构、管理制度、管理流程、人员管理、系统建设、系统运维等方面的安全性评估。

◆基于实施方式分类：按照网络安全测评的实施方式，测评主要包括：

1．安全功能检测。依据网络信息系统的安全目标和设计要求，对信息系统的安全功能实现状况进行评估，检查安全功能是否满足目标和设计要求。主要方法是：访谈调研、现场查看、文档审查、社会工程、漏洞扫描、渗透测试、形式化分析验证等。

2．安全管理检测。依据网络信息系统的管理目标，检查分析管理要素及机制的安全状况，评估安全管理是否满足信息系统的安全管理目标要求。主要方法是：访谈调研、现场查看、文档审查、安全基线对比、社会工程等。

3．代码安全审查。是对定制开发的应用程序源代码进行静态安全扫描和审查，识别可能导致安全问题的编码缺陷和漏洞的过程。

4．安全渗透测试。通过模拟黑客对目标系统进行渗透测试，发现、分析并验证其存在的主机安全漏洞、敏感信息泄露、SQL注入漏洞、跨站脚本漏洞及弱口令等安全隐患，评估系统抗攻击能力，提出安全加固建议。

网络安全测评类型

5．信息系统攻击测试。根据用户提出的各种攻击性测试要求，分析应用系统现有防护设备及技术，确定攻击测试方案和测试内容；采用专用的测试设备及测试软件对应用系统的抗攻击能力进行测试，出具相应测试报告。测试指标包括：防御攻击的种类与能力，如拒绝服务攻击、恶意代码攻击等。

◆基于测评对象保密性分类：按照测评对象的保密性质，网络安全测评可分为两种类型：
1．涉密信息系统测评。是依据国家保密标准，从风险评估的角度，运用科学的分析方法和有效的技术手段，通过对涉密信息系统所面临的威胁及其存在的脆弱性进行分析，发现系统存在的安全保密隐患和风险，同时提出有针对性的防护策略和保障措施，为国家保密工作部门对涉密信息系统的行政审批提供科学的依据。

2．非涉密信息系统测评。是依据公开的国家信息安全标准、行业标准、信息安全规范或业务信息安全需求，利用网络信息安全技术方法和工具，分析信息系统面临的网络安全威胁及存在的安全隐患，综合给出网络安全状况评估和改进建议，以指导相关部门的信息安全建设和保障工作。

网络安全测评流程与内容

◆网络安全等级保护测评内容：网络信息系统安全等级测评主要包括技术安全测评、管理安全测评。其中，技术安全测评的主要内容有安全物理环境、安全通信网络、安全区域边界、安全计算环境、安全管理中心；管理安全测评的主要内容有安全管理制度、安全管理机构、安全管理人员、安全建设管理、安全运维管理。

◆根据网络安全等级保护2.0标准规范，网络信息系统安全等级测评过程包括测评准备活动、方案编制活动、现场测评活动和报告编制活动四个基本测评活动。

◆网络安全渗透测试流程与内容：网络安全渗透测试的过程可分为委托受理、准备、实施、综合评估和结题五个阶段。
1．委托受理阶段。售前与委托单位就渗透测试项目进行前期沟通，签署“保密协议”，接收被测单位提交的资料。前期沟通结束后，双方签署“网络信息系统渗透测试合同”。

2．准备阶段。项目经理组织人员依据客户提供的文档资料和调查数据，编写制定网络信息系统渗透测试方案。项目经理与客户沟通测试方案，确定渗透测试的具体日期、客户方配合的人员。项目经理协助被测单位填写“网络信息系统渗透测试用户授权单”，并通知客户做好测试前的准备工作。如果项目需在被测单位的办公局域网内进行，测试全过程需有客户方配合人员在场陪同。

网络安全测评流程与内容

3．实施阶段。项目经理明确项目组测试人员承担的测试项。测试完成后，项目组整理渗透测试数据，形成“网络信息系统渗透测试报告”。

4．综合评估阶段。项目组和客户沟通测试结果，向客户发送“网络信息系统渗透测试报告”。必要时，可根据客户需要召开报告评审会，对“网络信息系统渗透测试报告”进行评审。如被测单位希望复测，由被测单位在整改完毕后提交信息系统整改报告，项目组依据“网络信息系统渗透测试整改报告“开展复测工作。复测结束后，项目组依据复测结果，出具“网络信息系统渗透测试复测报告”。

5．结题阶段。项目组将测评过程中生成的各类文档、过程记录进行整理，并交档案管理员归档保存。项目组质量工作人员请客户填写“客户满意度调查表”，收集客户反馈意见。

网络安全测评技术与工具

◆漏洞扫描：常用来获取测评对象的安全漏洞信息，常用的漏洞扫描工具有网络安全漏洞扫描器、主机安全漏洞扫描器、数据库安全漏洞扫描器、Web应用安全漏洞扫描器。

◆安全渗透测试：通过模拟攻击者对测评对象进行安全攻击，以验证安全防护机制的有效性。根据对测评对象掌握的信息状况，安全渗透测试可以分为三种类型。

1．黑盒模型。只需要提供测试目标地址，授权测试团队从指定的测试点进行测试。

2．白盒模型。需要提供尽可能详细的测试对象信息，测试团队根据所获取的信息，制订特殊的渗透方案，对系统进行高级别的安全测试。该方式适合高级持续威胁者模拟。

3．灰盒模型。需要提供部分测试对象信息，测试团队根据所获取的信息，模拟不同级别的威胁者进行渗透。该方式适合手机银行和代码安全测试。

◆代码安全审查：是指按照C、Java、OWASP等安全编程规范和业务安全规范，对测评对象的源代码或二进制代码进行安全符合性检查。典型的代码安全缺陷类型有缓冲区溢出、代码注入、跨站脚本、输入验证、API误用、密码管理、配置错误、危险函数等。

◆协议分析：用于检测协议的安全性。常见的网络协议分析工具有TCPDump、Wireshark。

◆性能测试：性能测试用于评估测评对象的性能状况，检查测评对象的承载性能压力或安全对性能的影响。常用的性能测试工具有性能监测工具（操作系统自带）、Apache JMeter（开源）、LoadRunner（商业产品）、SmartBits（商业产品）等。

网络安全测评质量管理与标准

◆网络安全测评质量管理：网络安全测评质量管理是测评可信的基础性工作，网络安全测评质量管理工作主要包括测评机构建立质量管理体系、测评实施人员管理、测评实施设备管理、测评实施方法管理、测评实施文件控制、测评非符合性工作控制、体系运行监督、持续改进。目前，有关测评机构的质量管理体系的建立主要参考的国际标准是ISO 9000。

◆中国合格评定国家认可委员会（简称CNAS）负责对认证机构、实验室和检查机构等相关单位的认可工作，对申请认可的机构的质量管理体系技术能力分别进行确认。

谢谢！