上海电力大学信息安全专业中本贯通

专业基础《渗透测试》考试大纲

一、考核目的

基于中本贯通教育考试指导意见，本次考试旨在考核学生是否达到了升入本科继续学习的要求。该专业课程旨在让学生掌握渗透测试工具和技术，熟悉渗透测试标准流程，即前期交互、信息收集分析、威胁建模、漏洞分析、渗透攻击、后渗透测试和渗透测试报告撰写。要求学生学会使用渗透测试工具来评估系统和网络的安全性，掌握漏洞分析和漏洞利用的能力。考查学生对于识别、分析系统及应用程序中的潜在漏洞、利用这些漏洞进行攻击等方面是否满足本科阶段的学习要求。

二、参考教材

1.《Kali Linux2 网络渗透测试实践指南》（第二版）李华峰主编 人民邮电出版社，2022 年
2.《Web 安全漏洞原理及实战》田贵辉 主编，人民邮电出版社，2020 年
3.《渗透测试基础教程》黄洪、尚旭光、王子钰 主编，人民邮电出版社，2019 年
4.《网络安全与攻防技术实训教程》（第二版）冼广淋、张琳霞主编，电子工业出版社，2018 年

三、考试内容及要求

1、渗透测试方法与流程

- 了解渗透测试的概念、特点；
- 了解白盒、黑盒、灰盒等方法在渗透测试中的应用；
- 了解渗透测试项目启动、准备、实施、汇报各阶段的工作内容；
- 了解渗透测试常用的工具；
- 了解渗透测试中风险规避的原则及常用措施；
- 了解渗透测试方案、报告等材料编写要点。

2、基础知识和技术

- 熟悉网络通信基础知识（如TCP/IP 协议）；
- 熟悉常见操作系统和网络设备的基础知识；
- 熟悉编程和脚本语言基础（如Python、Bash等）；
- 了解加密和解密技术基础。

3、信息收集分析

- 了解信息收集的概念及作用；
- 掌握公开信息收集的方法与技巧；
- 掌握端口扫描和服务发现技术；

- 了解漏洞信息库的查询方法；
- 了解社会工程学在信息收集中的应用。

4、漏洞扫描与评估

- 掌握自动化漏洞扫描工具的使用（如AWVS、Nmap等）；
- 熟悉手动漏洞评估技术；
- 掌握常见Web应用漏洞（如SQL注入、文件上传、文件包含、命令执行、XSS等）；
- 熟悉常见系统和网络漏洞（如缓冲区溢出、权限提升等）。

5、渗透攻击技术与利用

- 熟悉漏洞利用的原理和方法；
- 掌握常见的渗透攻击向量（如远程代码执行、文件包含等）；
- 熟悉提权技术和权限维持方法；
- 掌握实验环境下靶机渗透的方法。

6、后渗透测试技术与清理痕迹

- 掌握后门和持久性访问技术；
- 熟悉数据加密和隐匿传输技术；
- 了解日志清理和痕迹消除方法；

7、社会工程学攻击

- 了解社会工程学攻击的概念；
- 了解利用社会工程学直接攻击的方法；
- 了解社工库的概念及在网络攻击中的作用；
- 掌握社会工程学在口令破解中的利用方法；
- 了解应对社会工程学攻击的防御措施。

四、考试形式、题型和分值

1、考试形式：闭卷笔试，考试限定用时为 120 分钟。

2、题型和分值：选择题、判断题、填空题、简答题、综合题，满分为 150 分。