

2025 年全国硕士研究生招生试 国防科技大学自命题科目考试大纲

科目代码：F1007

科目名称：网络安全基础

一、考试要求

1. 了解网络空间、网络空间安全、网络攻击、网络防护等网络对抗相关概念；
2. 了解影响网络安全的因素，掌握网络体系结构的脆弱性、典型网络协议安全性、计算机系统安全性；
3. 掌握网络侦察基本概念、网络侦察技术原理与分类，了解网络侦察防御方法；
4. 了解网络扫描的基本概念，掌握主机发现、端口扫描、操作系统识别、漏洞扫描的原理；
5. 了解拒绝服务攻击基本概念，掌握拒绝服务攻击原理与分类，了解拒绝服务攻击的检测及响应技术；
6. 了解计算机病毒、计算机蠕虫、计算机木马基本概念，掌握木马的工作原理和隐藏技术；
7. 掌握口令猜测基本原理，熟悉操作系统口令破解、网络应用口令破解；
8. 了解网络监听基本概念，掌握网络监听基本原理、网络流量劫持分类与原理；

9. 了解缓冲区溢出攻击基本概念，掌握缓冲区溢出攻击原理、缓冲区溢出攻击防护；

10. 了解 Web 网站攻击技术基本概念、Web 应用体系结构脆弱性，掌握 SQL 注入攻击、跨站脚本攻击、Cookie 欺骗、CSRF 攻击的原理与防范；

11. 了解社会工程学基本概念，掌握社会工程常用技术及其原理，了解社会工程攻击防范等。

二、考试内容

1. 网络对抗相关概念，包括网络空间、网络空间安全、网络攻击、网络防护等基本概念；

2. 网络脆弱性分析，包括影响网络安全的因素、网络体系结构的脆弱性、典型网络协议安全性分析、计算机系统及安全性分析等；

3. 网络侦察技术，包括网络侦察基本概念、网络侦察方法、网络侦察防御方法；

4. 网络扫描技术，包括网络扫描的基本概念、主机发现、端口扫描、操作系统识别、漏洞扫描；

5. 拒绝服务攻击技术，包括拒绝服务攻击基本概念、拒绝服务攻击原理、拒绝服务攻击的检测及响应技术等；

6. 恶意代码技术，包括计算机病毒、计算机蠕虫、计算机木马基本概念，木马的工作原理和隐藏技术等；

7. 口令攻击技术，包括口令猜测、操作系统口令破解、网

络应用口令破解等；

8. 网络监听技术，包括网络监听基本概念、网络监听基本原理、网络流量劫持等；

9. 缓冲区溢出攻击，包括缓冲区溢出攻击基本概念、缓冲区溢出攻击原理、缓冲区溢出攻击防护等；

10. Web 网站攻击技术，包括 Web 网站攻击技术基本概念、Web 应用体系结构脆弱性、SQL 注入攻击及防范、跨站脚本攻击、Cookie 欺骗及防范、CSRF 攻击及防范等；

11. 社会工程学，包括社会工程学基本概念、社会工程常用技术、社会工程攻击防范等。

三、考试形式

考试采用闭卷方式进行笔试，考试时间为 2 小时。

总分为 100 分。具体题型及分值设置如表 1 所示。

表 1 网络安全基础考试试卷题型及分值设置

试卷内容	选择题	填空题	简答题	综合题
网络安全基础	30 分	20 分	20 分	30 分

四、参考书目

1. 《网络攻防原理与技术》（第 3 版），吴礼发、洪征、李华波 著，机械工业出版社，2021.06