信息安全专业《防火墙与入侵检测技术》考试大纲

一、考试的基本要求

《防火墙与入侵检测技术》是信息安全专业的一门专业课。本大纲适用于报考湖南警察学院相关专业的专升本入学考试。

本课程要求考生在掌握防火墙相关原理与技术，熟悉防火墙配置方法基础上，在 Windows 和 Linux 操作系统环境中针对不同网络特点恰当的布置防火墙。同时，要求考生正确理解入侵检测技术的相关概念，掌握入侵检测技术的类型、特点和发展趋势以及入侵检测技术的实现模型，将理论与实践有机结合，通过防火墙与入侵检测技术分析和解决网络安全中的现实问题。

二、考试的范围和内容

第 1 章 防火墙在网络安全防护中的地位和作用

1.考核知识点：

（1）开放系统互联参考模型 OSI

（2）TCP/IP 结构

（3）网络安全框架

2.考核要求：

（1）开放系统互联参考模型 OSI

识记：OSI 七层模型。

掌握：OSI 七层模型每一层的功能及其数据表现形式。

（2）TCP/IP 结构

掌握：①TCP/IP 每一层的功能及其数据表现形式。

②TCP、IP 与 UDP 头部结构；③TCP 三次握手过程。

（3）网络安全框架

识记：网络安全体系三维框架结构。

第 2 章 防火墙概述

1.考核知识点：

（1）防火墙定义和功能

（2）防火墙技术

（3）防火墙体系结构

（4）防火墙局限性

2.考核要求：

（1）防火墙定义和功能

识记：防火墙定义。

掌握：①防火墙三个基本性质；②边界防火墙功能；

③内部防火墙功能。

（2）防火墙技术

掌握：①包过滤原理，包过滤规则及包过滤策略；②

状态包过滤工作过程；③代理技术；④NAT 网络地址转换技术；⑤VPN 虚拟专用网技术。

应用：防火墙包过滤规则的设计。

（3）防火墙体系结构

识记：①四种防火墙体系结构。

（4）防火墙局限性

识记：①防火墙局限性。

第 3 章 防火墙技术要求

1.考核知识点：

（1）防火墙的等级划分

（2）功能要求

（3）性能要求

（4） 安全要求

（5）保证要求

2.考核要求：

（1）防火墙的等级划分

识记：①防火墙的等级划分依据。

（2）功能要求

识记：①一级、二级、三级防火墙产品功能要求的区别。

（3）性能要求

识记：防火墙的性能指标。

（4） 安全要求

识记：①一级、二级、三级防火墙产品安全要求的区别。

（5）保证要求

识记：①一级、二级、三级防火墙产品保证要求的区别。

第 4 章 防火墙测评方法

1.考核知识点：

（1）功能测试

（2）性能测试

（3）安全测试

（4）保证要求测试

2.考核要求

（1）功能测试

掌握：①防火墙功能测试方法。

（2）性能测试

掌握：①防火墙性能测试环境、工具和测试方法。

（3）安全测试

掌握：①防火墙安全测试方法。

（4）保证要求测试

掌握：①防火墙保证要求测试方法。

第 5 章 个人防火墙应用

1.考核知识点：

（1）Windows 防火墙设置与应用

2.考核要求：

（1）Windows 防火墙设置与应用

掌握：①Windows 防火墙启用与禁用方法；②管理与添加防火墙“例外”；③ Windows 防火墙基本设置；④创建入站规则和出站规则；⑤查看和管理规则。

应用：Windows 防火墙规则的设置。

第 6 章 开放防火墙 Linux iptables 应用

1.考核知识点：

（1）netfilter

（2）iptables

2.考核要求：

（1）netfilter

识记：①netfilter 功能；②netfilter 中的表。

掌握：netfilter 数据包处理流程。

（2）iptables

识记：①iptables 命令的格式；②iptables 命令的选项和参数。

掌握：①iptables 规则的设置方法。

应用：实际网络环境中 iptables 规则的设计。

第 7 章 入侵检测概述

1.考核知识点：

（1）网络安全基本概念

（2）入侵检测的产生与发展

（3）入侵检测基本概念

2.考核要求：

（1）网络安全基本概念

识记：①网络安全的基本特征。

掌握：①P2DR 模型；②P2DR 模型时间值描述方法。

（2）入侵检测的产生与发展

识记：①入侵检测的发展历程。

（3）入侵检测基本概念

识记：入侵检测概念。

第 8 章 入侵方法与手段

1.考核知识点：

（1）网络入侵

（2）漏洞扫描

（3）拒绝服务攻击

（4）分布式拒绝服务攻击

（5）缓冲区溢出攻击

2.考核要求：

（1）网络入侵

识记：网络入侵的一般流程。

（2）漏洞扫描

掌握：①漏洞扫描方法。

（3）拒绝服务攻击

掌握：①拒绝服务攻击原理；②典型拒绝服务攻击的

手段。

（4）分布式拒绝服务攻击

掌握：①分布式拒绝服务攻击原理。

（5）缓冲区溢出攻击

掌握：缓冲区溢出攻击原理。

第 9 章 入侵检测系统

1.考核知识点：

（1）入侵检测系统基本模型

（2）入侵检测系统分类

2.考核要求：

（1）入侵检测系统基本模型

掌握：通用型、层次化和管理式入侵检测模型。

（2）入侵检测系统分类

掌握：入侵检测系统分类方法。

第 10 章 入侵检测流程

1.考核知识点：

（1）入侵检测过程

（2）入侵检测系统数据源

（3）入侵检测的分析方法

（4）告警与响应

2.考核要求：

（1）入侵检测过程

识记：①入侵检测过程 3 个阶段。

（2）入侵检测系统数据源

识记：①入侵检测系统主机与网络数据源。

（3）入侵检测的分析方法

掌握：①误用检测与异常检测方法；②误用检测与异常检测方法的区别。

（4）告警与响应

掌握：①响应类型。

第 11 章 基于主机的入侵检测技术

1.考核知识点：

（1）审计数据的获取

（2）基于主机的入侵检测技术

2.考核要求：

（1）审计数据的获取

掌握：①审计数据的获取与数据预处理方法。

（2）基于主机的入侵检测技术

掌握：①基于主机的入侵检测技术中的各种技术方法。

第 12 章 基于网络的入侵检测技术

1.考核知识点：

（1）网络数据包的获取

（2）检测引擎的设计

2.考核要求：

（1）网络数据包的获取

掌握：①数据包的捕获技术。

（2）检测引擎的设计

掌握：①检测引擎的设计方法；②网络入侵检测特征的选取方法。

第 13 章入侵检测系统的标准与评估

1.考核知识点：

（1）入侵检测的标准化工作

（2）入侵检测系统的性能指标

2.考核要求

（1）入侵检测的标准化工作

掌握：①入侵检测系统 CIDF 框架。

（2）入侵检测系统的性能指标

识记：①入侵检测系统检测率、虚警率、漏警率。

掌握：①ROC 曲线评价入侵检测系统性能的方法。

三、考试题型和分值结构（100 分）

考试题型共五种：单选题（20 分）、多选题（15 分）、填空题（20 分）、判断题（10 分）、简答题（20 分）、设计题（15 分）。

四、考试形式

笔试（闭卷）

五、考试时间

120 分钟

六、主要参考书目

[1] 陈波,于泠. 防火墙技术与应用（第 2 版）.北京：机械工业出版社，2021 年 10 月.

[2] 薛静锋,祝烈煌.入侵检测技术（第 2 版）.北京：人民邮电出版社，2016 年 1 月.