附件

2019年全国信息安全管理员

知识与技能竞赛内容大纲

第一部分 信息安全管理员重点理论知识

网络安全员理论基础知识涵盖以下内容：一是《网络安全法》等相关法律法规；二是中国人民公安大学出版社2018年4月出版的全国信息网络安全专业技术人员继续教育基地培训用书，包括《网络安全管理实践》、《信息安全技术》、《网络安全合规指引》3本；三是其它网络安全相关知识。

要求竞赛选手比较系统地掌握上述专业知识的基本概念、基本原理和基本方法，能够综合运用相关基本原理和基本方法分析、判断、解决网络安全相关实际问题。

第二部分 信息安全管理员重点技能要求

|  |  |  |  |
| --- | --- | --- | --- |
| 序号 | 模块 | 方 向 | 技能要点 |
| 1 | 基础安全模块 | 网络协议分析 | TCP/IP协议分析、HTTP协议分析、其他常见网络协议分析 |
| 网络安全设备 | 防火墙安全配置、IDS安全配置、IPS安全配置、漏洞扫描设备安全配置、WAF安全配置、其他网络安全设备安全配置 |
| 常见网络攻击及防护技能 | 信息泄露攻击及防护、网站访问类攻击及防护、拒绝服务攻击及防护、其他常见攻击及防护 |
| 常用工具的使用 | 网络诊断工具、系统监控工具、漏洞扫描工具、流量分析工具、信息收集工具 |
| 主机安全基础知识 | 访问控制、安全审计、入侵防范、恶意代码防范 |
| 2 | 运维保障模块 | 系统安全 | 主机安全配置，日志审计，应用、web框架、中间件安全，系统漏洞补丁管理，恶意代码（木马、病毒、挖矿、蠕虫），系统权限控制，系统资源监控 |
| 网络安全 | 端口防护，防DDOS、防扫描相关技术，网络隔离，常用网络设备配置与安全加固 |
| 应用安全 | 应用系统防逆向、防篡改（app和网站），网页防暗链，防钓鱼 |
| 数据安全 | 数据备份、数据加解密、数据传输安全 |
| 3 | 应急处置模块 | 网络安全事件分析 | 识别网络安全事件、网络安全事件响应、网络安全事件溯源 |
| 入侵检测及防御 | 入侵行为检测、流量分析与监测、数据分析 |
| 日志审计分析 | 系统日志分析、应用日志分析、数据库日志分析、安全产品日志分析 |
| 安全隐患排查（系统和网络） | 渗透测试、基线检查、系统漏洞、安全加固 |
| 应急处置与取证工具 | 应急处置方法、应急处置流程、应急处置与取证工具综合应用 |