ISC 2017

2017 中国互联网安全大会 China Internet Security Conference

新形势下应急响应的人才需求

位华 中国信息安全测评中心

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

重大网络安全事件频发

乌克兰电力系统遭受攻击事件

2015年12月23日，乌克兰电力部门遭受到恶意代码攻击，“至少有三个电力区域被攻击，并于当地时间15时左右导致了数小时的停电事故”；“攻击者入侵了监控管理系统，超过一半的地区断电几个小时。”

希拉里邮件门事件

希拉里被曝担任国务卿期间使用私人电子邮箱与他人通信,涉嫌违反美国《联邦档案法》。在希拉里的大量邮件中，其中有十多封邮件涉及到“最高机密”。希拉里邮件门事件影响甚大，假如邮件遭到泄露，将对国家安全造成非常严重的破坏。邮件门事件本身也直接影响了美国大选的最终结果。

WannaCry勒索事件病毒

WannaCry勒索（永恒之蓝）事件病毒，已波及100多个国家和地区10万台电脑被感染，已经有100多个国家遭受了攻击，其中包括英国、美国、中国、俄罗斯、西班牙和意大利。迅速向全球扩散的勒索病毒网络攻击受害者还会继续增加，因为黑客可以轻松进入那些几个月没有更新微软公司“视窗”操作系统的电脑中。

面对安全事件我们该如何应对？

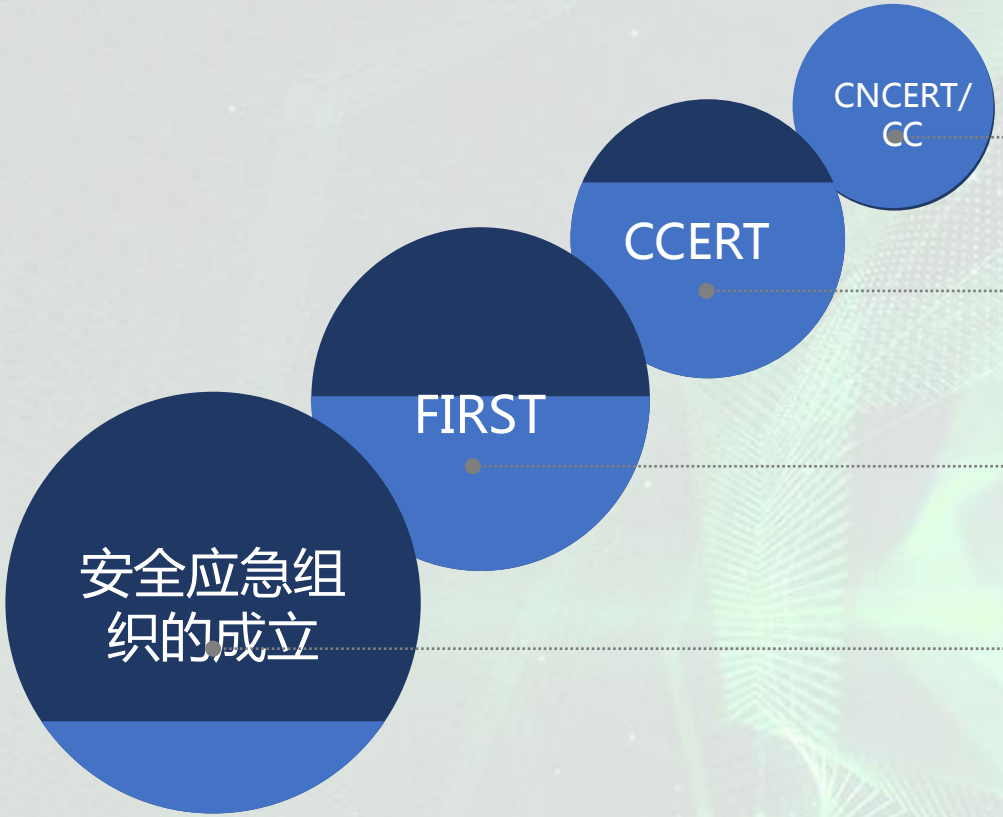
- 计算机病毒入侵造成客户信息业务系统数据外泄、篡改、删除破坏严重安全威胁。
- 网络攻击造成客户信息业务系统中断，给客户业务运转造成严重经济业损失。

- 网站挂马降低公众信誉度，影响客户行业公众形象，挂马使网站成为木马传播的帮凶。
- 面对安全威胁如何建立快速、有效、完备的安全事件处置机制

引入专业应急响应团队

以应急服务的形式邀请专业安全团队处理突发的安全事件

安全应急响应发展过程



2002年，CNCERT/CC加入FIRST。

1999年中国第一个应急响应组织在清华大学成立。

于1990年11月成立了国际“计算机事件响应与安全工作论坛”(FIRST)组织。

源于莫里斯蠕虫案件，1989年，美国国防部、国家安全局及国防通信局相继成立了安全应急组织。

应急响应处理机制

1. 建立应急处理机制或体系。
2. 制定最高当局主导、全社会参与的应急法律或规章。
3. 确立应急处理预警等级。
4. 建立应急处理队伍，实行7天×24小时值勤。

应急响应服务的关键

应急响应服务的主要内容

- 检查安全事件来源。
- 恢复系统正常工作。
- 安全事件深度分析。
- 发布安全事件通告。
- 提供系统风险评估。

人是安全的尺度

加强专业应急安全人才队伍的建设是应对频发安全事件的关键要素。

应急响应服务的关键

数据分析能力

通过安全审计和日志数据来分析和发现网络存在的未知或者未发现的攻击。

安全逆向能力

有较好的逆向思维能力，熟练使用各种分析工具和渗透测试工具。

安全实践能力

熟悉常见网络攻击手段及验证方法，如：Web安全、移动安全、系统网络。

网络基础知识

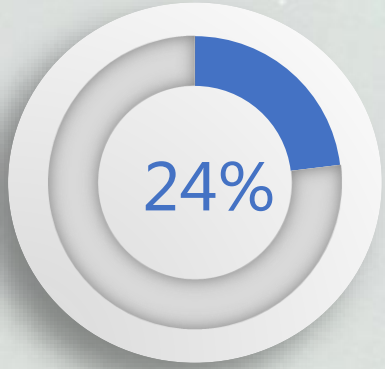
掌握扎实的安全基础知识，包括网络、系统、应用等领域。

ISC 2017 中国互联网安全大会

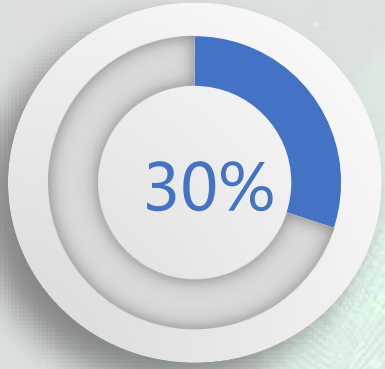
360互联网安全中心

目录

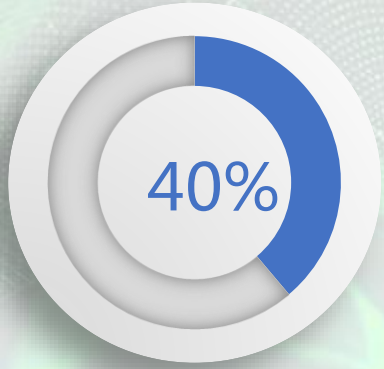
国内企业安全团队建设情况



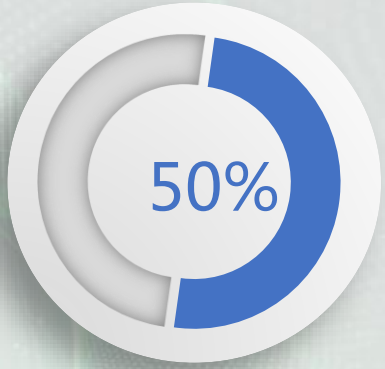
24%的企业没有信息安全团队。



30%的企业每年基本上没有信息安全预算。

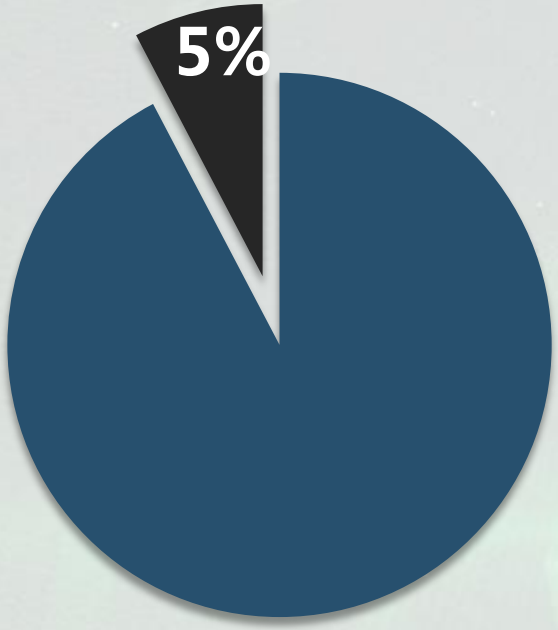


40%的小微企业(100人以下)没有信息安全团队和资金预算。



超过50%的金融企业没有安全团队建设的投入。

安全人才缺口巨大



国内安全人才缺口高达95%

近年我国高校教育培养的信息安全专业人才仅3万余人，而网络安全人才总需求量则超过70万人，缺口高达95%

安全人才缺口巨大

全球性问题

专业保险商Hiscox Insurance最新发布的报告显示，美国、英国和德国只有不足半数的企业做好了应对网络攻击的准备。网络安全形势日益严峻，如何弥合人才的巨大缺口，成为国家和安全产业面临的一大难题。

人才培养政策

中网办
（2016）
4号文

01 加快网络安全学科专业和院系建设。

02 创新网络安全人才培养机制。

.....

07 加强全民网络安全意识与技能培养。

08 完善网络安全人才培养配套措施。。

人才培养过程中遇到的问题

课程落后

截至**2016**年，教育部批准全国共**109**所高校设置信息安全类相关本科专业，培养信息安全类专业本科毕业生超过**1**万人**/**年 ，信息安全专业的课程大部分为高等数学、线性代数、计算方法、概率论与数理统计、计算机与算法初步、C++语言程序设计、数据结构与算法等传统计算机专业教程。

缺乏实战

无论是高校信息安全专业的毕业生，还是专业培训机构学员大多数缺乏安全攻防实战的经验。

ISC 2017 中国互联网安全大会

360互联网安全中心

目录

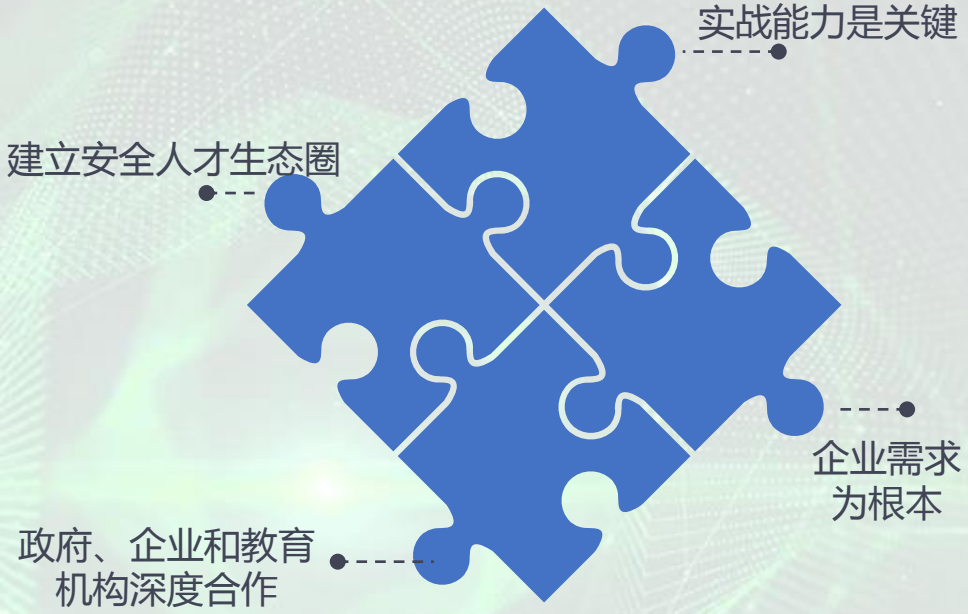
沙场才能点兵

ISC 2017 中国互联网安全大会

360互联网安全中心

应急响应人才培育模式

1. 选择有社会责任感的安全企业深度参与安全应急响应人才的培养，并参与人才资质认证考试。
2. 教育理念创新，编写新的课程培养专业技术人才。
3. 国家相关机构发挥的带头作用，制定专业安全人才培养方向，并对人才进行标准化的能力认证。
4. 提高学生的安全应急响应实践技术能力。



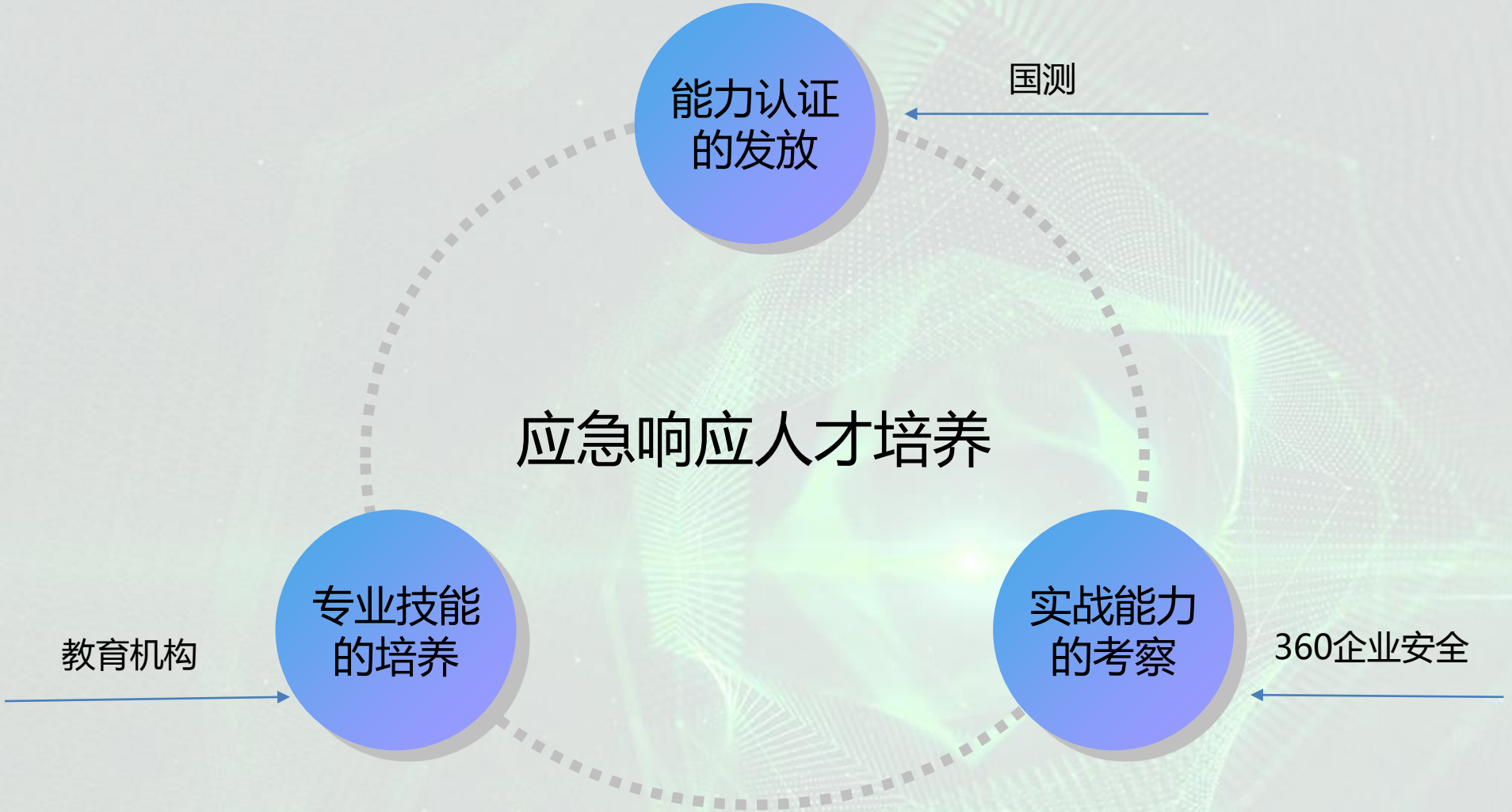
人才培养生态圈

政府负责调研统计安全人才缺口、专业技能需求，制定人才培养方向、职业技能的认证。

高校（专业培训机构）负责知识的传递、专业技能的培训。

企业参与人才的选拔、技能的认证，并给合格的人才提供就业的岗位。

生态圈紧耦合良性循环



ISC 2017 中国互联网安全大会

360互联网安全中心

目录

考试简介

考试是为了锻炼考生实际解决网络安全问题的能力，有效增强我国网络安全防御能力，促进国家企事业单位网络防御能力不断提高，以发现人才，选拔优秀人才而设立的技能水平考试。

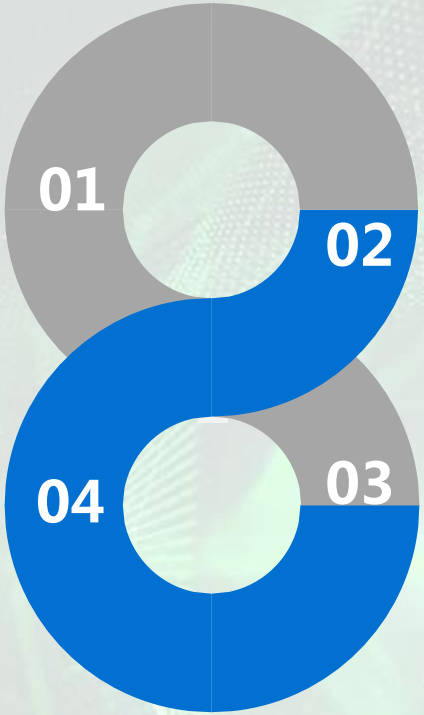
考试内容从多个角度出发，客观题与实操题相结合的形式，来考核考生的能力，通过多个得分点，对考生全面的考核，考生需要了解最新的网络安全技术，跟踪最新的网络安全动态，能够在真实的网络环境中发现问题和解决问题。也可以为网络安全专业的学生提高自身价值，提高自身影响力，提供更好学习素材。

攻防领域专家注册考试

考试方向

Web安全基础

了解HTTP协议基础，以及一些常见的web安全漏洞包括注入漏洞，XSS漏洞，CSRF漏洞，SSRF漏洞，文件处理漏洞，访问控制漏洞，会话管理漏洞。考生应该能够理解和发现这些漏洞，并且学会修复这些漏洞的方法，掌握更多的安全技术。



中间件安全基础

包括Apache,IIS,Tomcat,以及JAVA开发的中间件Weblogic,Jboss, Websphere等。了解中间件的特性以及安全加固的方法，避免在安全设置上产生安全问题影响整个安全体系，了解最新的安全漏洞，能够对最新的漏洞做出响应，提高整体安全标准。

服务器安全基础

包括Windows,Linux操作系统账户的分配与安全设置，文件系统权限的管理，日志审计的基本方法，以及第三方应用安全。由此可以加强考生对操作系统安全的理解，了解常见的攻击手段，以及操作系统安全加固的基础知识，通过日志审计进行安全事件分析，掌握最新的系统内核漏信息，能够及时修复漏洞，提高操作系统的安全性能。

数据库安全基础

以Mssql,Mysql,Oracle,Redis数据库为主，了解数据库的使用方法和语法结构，掌握数据库的安全设置以及权限，角色的分配。了解常用的利用数据库来进行文件操作和权限提升的方法以及应对措施，控制数据库运行权限，保证数据库中的数据完整和安全运营。

攻防领域专家注册考试

— 考生收益 —

增加个人优势

由于CISP-PTE是技能水平证书，表明了通过考试的学员拥有在职场中直接上岗独当一面工作的能力。因此在求职时有自己的优势。

增加薪资

由于CISP-PTE考试形式主要以实操为主，充分考核了考生的在企业安全中遇到的网络安全问题，因此证书含金量颇高，是薪资谈判时的重要砝码。

学习能力

人力资源专家和猎头们普遍认为，证书的取得的目标在于要不断充实自己。在这个知识更新越来越快的终身学习时代，可以向企业表明自己具有学习能力，而且有意识地在不断充实自己。。

攻防领域专家注册考试

— 考试形式 —

Web安全基础答题

安全加固与防御答题与实操

渗透测试实操考试

日志与数据分析实操考试

攻防领域专家注册考试

——考试内容与考核要求——

知识类	章节	考核标准
		内容
WEB安全基础	HTTP协议	HTTP协议基础知识
	注入漏洞	SQL注入的基础知识
		XML实体注入基础知识
		RFI远程文件包含漏洞的原理和修复方法
		LFI 本地文件包含漏洞的原理和修复方法
		RCE远程代码执行漏洞的原理和修复方法
	XSS漏洞	存储型XSS漏洞发现与防范
		反射型XSS漏洞发现与防范
		Dom型XSS漏洞发现与防范
	CSRF漏洞	CSRF跨站请求伪造漏洞的分析与利用
	SSRF漏洞	SSRF服务端请求伪造漏洞的分析与利用
	文件处理漏洞	任意文件上传漏洞产生的原因与修复方法
		任意文件读取漏洞产生的原因与修复方法
	访问控制漏洞	垂直越权漏洞的分析与利用
		水平越权漏洞的分析与利用
	会话管理漏洞	会话固定漏洞的产生原因和防范
		会话劫持漏洞的产生原因和防范
		Cookie欺骗漏洞的产生原因和防范

知识类	章节	考核标准
		内容
中间件安全	Apache	Apache 服务器权限配置
		Apache 服务器文件解析漏洞
		Apache 服务器日志审计方法
		Apache 服务器Web目录权限的设置
	IIS	IIS6文件解析漏洞利用
		IIS6写权限漏洞的利用
		IIS6短文件名漏洞
		IIS7 FastCGI方式调用PHP存在的解析漏洞
		IIS日志审计方法
	Tomcat	Tomcat 管理账号密码修改方法
		Tomcat 通过后台获取权限的方法
		Tomcat 服务器启动权限设置
		Tomcat 日志审计方法
	Weblogic	Weblogic 反序列化漏洞
		Weblogic 管理后台弱口令风险
		Weblogic 服务端请求伪造漏洞
		Weblogic 日志审计方法
	JBoss	JBoss 反序列化漏洞
		JBoss jmx-console/web-console 未授权访问
		JBoss jmx Invoker 远程命令执行
		JBoss 日志审计方法
	Websphere	Websphere 账号管理授权
		Websphere 反序列化漏洞
		Websphere 管理后台弱口令风险
		Websphere 日志审计方法

攻防领域专家注册考试

——考试内容与考核要求——

知识类	章节	考核标准
		内容
操作系统安全	Windows系统安全	账户密码弱口令风险
		账户的分组和权限
		NTFS 文件系统权限的设置
		Windows日志的种类和审计方法
		第三方应用和服务存在的漏洞
		Windows权限提升方法
	Linux系统安全	检查用户空口令的方法
		设置账户认证失败锁定次数和时间
		检查除root以外的UID为0的用户
		查找系统中存在的SUID和SGID程序
		查找任何人都有写权限的目录和文件
		第三方应用和服务可能存在的漏洞
		Linux权限提升方法
		系统日志的分类和审计方法

知识类	章节	考核标准
		内容
数据库安全	Mssql数据库安全	Mssql数据库的查询语法
		Mssql数据库账户密码存在弱口令的风险
		Mssql数据库服务器启动权限的设置
		Mssql数据库的角色与权限的分配
		Mssql数据库中常用的存储过程
		Mssql数据库备份和日志备份方法
		Mssql存储过程提权的方法
	Mysql数据库安全	Mysql数据库的查询语法
		Mysql账户密码弱口令风险
		Mysql创建用户并指定数据库授权
		Mysql读取文件和导出文件的方法
		Mysql提权的方法
	Oracle数据库安全	Oracle数据库的查询语法
		Oracle数据库执行系统命令的方法
		Oracle数据库账号权限的分配
		Oracle数据库账号密码策略配置
		Oracle数据库日志审计
	Redis数据库安全	Redis 数据库未授权访问的危害
		Redis 数据库启动权限的设置
		Redis 写入文件的方法

谢谢!