Web漏洞原理	《众元》安全攻防大师v9.1				
注象性別 3	能力目标	课程目标			
数通网络技术 80 無過网络基础、地址规划、协议基础、协议安全成熟、网络设备调点、路由协议、TCP/IP 编程语言基础 30 期悉时间标识、php函数、sqi语句、python使用等 Linux系统 30 期悉基本命令、vim的操作、文件的操作等 数据库基础 18 無悉数銀库语法、操作数据库、数据表、DBMS 参及工作。xss、文件解析、框架漏洞、命场行、优码执行、csrf、ssrf、xve、反序列化、中间件通讯 解析漏洞、数据库漏洞、超权漏洞、信息避避等 OWASP Topa漏洞 web漏洞发现与利用 30 熟悉调工具AWVS等使用、webshell的利用、致创等 代码审计 30 熟悉则内代码、jr代码、Java代码审计,审计工 权限提升 30 熟悉Windows、Linux的摄权方法等 笔试+top企业渗透测试岗位面试要求 第三式+top企业渗透测试岗位面试要求 第三式+top企业渗透测试岗位面试要求 第三式和wp 20 题表参及有限 30 熟悉则有效的 20 题表参加,可能力能和wp 20 题表参加,可能力能和 30 题表参加,可能力能和 30 题表参加,对能力的位面式要求 第三进制即的 120 题表参加,对能力的位面式要求 第三进制即的 120 题表表值,C、栈溢出,格式化字符、栈溢出漏 测定解析 30 题表表值,C、栈溢出,格式化字符、栈溢出漏 测定解析 30 题表表值,从表面,对于解几种加密方式、数据交易能力,对解几种加密方式。 第一进的工具和解密算法等解题方法和wp 第一类中国的 30 解题方法和wp 第一类中国的 20 解题方法和wp 第一次中国 20 解题方法和wp 第一次中国 20 解题方法和wp 第一次中国 20 解题方法和wp 第一次中国 20 解题方法和wp 20 解题方法和wp 第一次中国 20 解题方法和wp 20 解题方式和wp 20 解题 20 和 20					
安成時、		法律法规	3		
##程语言基础 30 用等		数通网络技术	80	全威胁、网络设备调试、路由协议、TCP/IP	
		编程语言基础	30		
Web Manage		Linux系统	30	熟悉基本命令、vim的操作、文件的操作等	
Web漏洞原理	渗透测试	数据库基础	18	熟悉数据库语法、操作数据库、数据表、DBMS	
Web漏洞发现与利用 30 飲働等 100 10	4	web漏洞原理	120	中间件漏洞、解析漏洞、数据库漏洞、越权漏洞	
大阪保護子 12 大阪保護子 13 大阪保護子 14 大阪保護子 14 大阪保護子 15 大	* _	web漏洞发现与利用	30	* * * * * * * * * * * * * * * * * * * *	
Web方向 60		代码审计	30	熟悉php代码、js代码、Java代码审计,审计工具	
CTF 完養 web方向 60 熟悉WEB+大安全漏洞 (OWASP Top 10) 等態		权限提升	30	熟悉Windows、Linux的提权方法等	
Time	阶段考核	笔试+t	op企业渗透	测试岗位面试要求	
Time		\sim			
CTF竞表 二进制pwn 120 洞等解题方法和wp 一遊向reverse 30 熟悉静态分析、动态分析,了解几种加密方式、熟悉安卓脱壳等解题方法和wp 空码学crypto 30 了解古典密码和熟悉使用解密工具和解密算法等解题方法和wp 杂项misc 30 熟悉流量分析、压缩包、图片障写、音频障写等解题方法和wp Src概念 3 了解src意义和排名机制 src平台 6 注册CNVD、补天、漏洞盒子、教育漏洞报告平台,挖洞 家rc平台 12 熟悉使用资产测绘引擎、企业信息查询、域名信息查询、域名信息查询 技掘技巧 12 了解绕过方式、某迅万能下载等 1/nday利用 12 了解漏洞文库收集,关注并使用最新漏洞 内网渗透基础 12 了解工作组、域、域环境、安全域的划分、资源、跳板等 数表frotb网络漆。portwd端口转常、venomefe 熟悉作成网络漆。portwd端口转常、venomefe		web方向	60	熟悉WEB十大安全漏洞(OWASP Top 10)等解题方法和wp	
逆向reverse 30 熟悉安卓脱売等解题方法和wp		二进制pwn	120		
密码学crypto 30 解题方法和wp 熟悉流量分析、压缩包、图片隐写、音频隐写 等解题方法和wp	CTF竞赛	逆向reverse	30		
杂项misc 30 等解题方法和wp SRC 赏金 SRC 赏金 SRC 赏金		密码学crypto	30	了解古典密码和熟悉使用解密工具和解密算法等解题方法和wp	
SRC 党金		杂项misc	30		
SRC 党金					
SRC 赏金 家rc 平台 6 平台,挖洞 素素使用资产测绘引擎、企业信息查询、域名信息查询 12 熟悉使用资产测绘引擎、企业信息查询、域名信息查询 挖掘技巧 12 了解绕过方式、某迅万能下载等 1/nday利用 12 了解漏洞文库收集,关注并使用最新漏洞 内网渗透基础 12 了解工作组、域、域环境、安全域的划分、资源、跳板等 熟悉frn内网穿透、portwd端口转发、venomefe 即来frn内网穿透、portwd端口转发、venomefe		src概念	3	了解src意义和排名机制	
おおけい おおけい おおけい おおけい おおけい おおけい おおけい おおけい まままます おおけい ままままます ままままます まままままます おおけい まままままます おおけい ままままます まままままます ままままままます まままままままま	CDC告令	src平台	6		
1/nday利用 12 了解漏洞文库收集,关注并使用最新漏洞 内网渗透基础 12 了解工作组、域、域环境、安全域的划分、资源、跳板等		src信息收集	12		
1/nday利用 12 了解漏洞文库收集,关注并使用最新漏洞		挖掘技巧	12	了解绕过方式、某迅万能下载等	
内网渗透基础 12 了解工作组、域、域环境、安全域的划分、资源、跳板等			12	了解漏洞文库收集,关注并使用最新漏洞	
内 図 内 図 方、 資源、 跳板等					
· · · · · · · · · · · · · · · · · · ·		内网渗透基础	12		
穿透与转发 12 理转发、多级穿透、DNS隧道		穿透与转发	12	熟悉frp内网穿透、portwd端口转发、venom-代 理转发、多级穿透、DNS隧道	

		4.0	熟悉端口扫描、口令爆破、主机信息收集、数据			
渗透测试进阶	内网信息收集	12	库信息收集、数据分析			
	通道构建	12	判断目标以哪种协议出网、反向代理、正向代理 、使用socks代理			
	权限提升	12	熟练Windows提权、Linux提权、本地提权、 web提权、数据库提权等			
	横向渗透	12	熟练在 windows 中进行横向移动、利用数据库 进行横向移动、使用 cs 进行横向移动的常用命令			
	权限维持	6	熟练windows 中的权限维持、linux 的权限维持 、数据库中的权限维持			
	痕迹清理	6	熟练防止恢复删除的文件、windows 的痕迹清理 、linux 的痕迹清理等方法和工具			
77	域渗透	18	熟练域基础、域信息收集、域权限利用、 域横向攻击			
	小程序app渗透	30	熟练微信小程序、 手机 app、程序流量分析			
	API渗透	18	熟练API 扫描、API 利用			
	Java安全	12	熟悉Java 基础、Spring Boot 框架、 Redis MongoDB 数据库等java架构安全威胁			
	13/5					
	蜜罐技术	6	熟悉蜜罐的分类及搭建部署,微步在线、低、中 、高蜜罐等			
	流量分析	18	熟悉使用Wireshark、Wireshark的功能过滤			
护网蓝队 (防守方)	攻击研判	18	熟悉设备监控: IPS 告警、WAF 告警、流量分析 告警终端防护告警; 事件上报: 保留证据、事件报告、上报处置; 后期处置: 协助处理、情报联动、攻击溯源			
	溯源	18	熟悉攻击源捕获,溯源反制手段,获取攻击者 信息			
	取证	12	熟悉webshell数据表、日志分析			
护网红队 (攻击方)	资产收集	12	熟悉工具的使用、端口服务、子域名、 C段旁站等报告模板整理			
	外网打点	12	熟练使用工具发现脆弱点、使用工具检测漏洞 并利用			
	蜜罐识别	6	熟悉蜜罐分类、如何识别蜜罐、常见蜜罐、 交互蜜罐等			
	社工钓鱼	18	熟悉社交账号、免杀马、bypass沙箱、信息收集 C2搭建、邮件网关等			
	内网渗透	18	熟练内网渗透基础、穿透与转发、内网信息收集 通道构建、权限提升、横向渗透、权限维持 痕迹清理、域渗透等			
	免杀对抗	12	熟悉免杀shellcode制作,免杀软件测试			
阶段考核	笔试	+护网行动组	工/蓝队面试要求			
	等级保护标准	6	熟悉等级保护介绍、等级保护的一般流程 等级保护 2.0 安全设备			

	内网安全部署	30	熟悉AAA 服务器技术及设备安全管理、LAN 接入基本安全、身份认证技术、网络准入控制 NAC、桌面云安全、EDR 终端检测响应技术
	公网边界防火墙部署	30	熟悉防火墙的工作层次、下一代防火墙概述 下一代防火墙组网方案、终端安全检测和防御技术、服务器安全检测和防御技术、防火墙技术 产品选型
安全合规保护	公网边界上网行为管理部署	18	熟悉上网行为安全概述、上网行为组网方案、 用户认证技术、应用控制技术、内容审计技术
	数据中心 WAF部署	18	熟悉web 应用防火墙概述、web 应用防火墙基本原理、web 应用防火墙部署模式
	总部与分支VPN互联	30	熟悉VPN 基础、IPSEC 的安全基础前篇、IPSEC 的安全基础后篇、IKE 工作过程、IPSEC 配置应用案例分析、SSL 移动接入方案、移动资源发布
45	安全运维	6	熟悉持续监控、事件管理和响应、漏洞管理、 配置管理、日志管理、策略管理
	研判告警	6	熟悉设备监控、事件上报、后期处理
安全(服务) 运营	应急响应	6	、文件痕迹排查、日志分析、内存分析、流量分 析
	威胁情报	6	熟悉威胁情报的基本特征、用途、数据采集 分析方法、服务平台等
	联动处置	3	熟悉处理流程和标准
阶段考核	笔试+安全工	程师及安全	运营工程师岗位面试要求
		A Second	\ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
呈现表达能力	PPT制作	6	熟练使用工具制作PPT
	台风界面训练	18	《我的家乡》演讲、《就业企业介绍》演 讲
	演讲技能及应变	30	《技术讲解》演讲、《产品选型》演讲、 《方案设计》演讲
			· 61
面试就业能力	就业课程	18	网络安全行业介绍、网络安全企业介绍 如何做好《自我介绍》、如何写好《个人简历》
	就业能力考核和辅导	30	就业能力考核、模拟面试及辅导、面试跟踪与辅 导
就业考核	简朋	5制作通过、	人事面试通过