		We like
- 4.3		蚁景网安渗透测试(红队方向)课程体系
课程分类	课程大纲	内容概述
渗透测试介绍	网络安全、渗透测试概念 渗透测试法律法规	渗透相关概念、基本流程、网安重大事件、安全意识介绍 网络安全法、反间谍法、渗透测试规范、授权渗透
	渗透测试就业前景、岗位及发展	网安相关岗位、hw、src、众测、就业需求、行业前景
	基础环境安装	windows系统配置、python环境、java环境
	VM虚拟机	Vmware软件安装与激活、VM虚拟网络编辑与配置
	Kali Linux 基础 Kali Linux 进阶	Kali Linux简介、Linux目录结构、文件属性、VIM编辑器、目录管理、网络配置、用户配置 Linux服务管理、防火墙、APT使用、Git使用、SSH使用、Kali工具
操作系统基础	内网靶场搭建	多层内网环境搭建、多层内网配置
		VPS介绍
	云服务器	云服务器对比与选购、VPS连接与使用
	docker	docker简介、docker安装与配置 docker搭建漏洞靶场、docker-compose搭建漏洞靶场
1/4° - 00°		docker/拾建瀰洞靶场、docker-compose拾建瀰洞靶场 网络协议分层
	计算机网络基础	IP地址、DNS、ARP、DHCP、NAT、ICMP
计算机网络		burpsuite安装、浏览器代理配置、证书配置
	计算机网络安全应用	burpsuite-proxy模块使用
		http协议、http报文分析、http请求方法、https与http 信息收集分类
	域名信息收集	域名介绍、域名收集、子域名收集
信息收集	IP信息收集	IP收集、C段
旧心収果	117日志収果	端口收集、常见端口及安全隐患介绍
	网站信息收集	操作系统收集、网站服务、容器收集、数据库识别、CMS识别
37-8		敏感文件、目录、常见WAF识别 wamp搭建靶场
	基础环境搭建	1amp搭建靶场
		docker、docker-compose搭建靶场
		Mysql基础
	SQL注入	SQL注入原理、危害、判断与分类 SQL注入显错注入、盲注、报错注入
		SQLmap使用实例及参数详解
		文件上传漏洞原理、危害、检测方式常见
		webshell简介、原理
web安全	文件上传	webshell管理工具,菜刀、蚁剑、冰蝎、哥斯拉 文件上传绕过方式、绕过js、绕过文件后缀检测、mime类型、绕过文件内容检测
		文件上传访御
		常见解析漏洞
		命令执行漏洞原理
	命令执行	php代码执行、命令执行函数 命令执行漏洞实例,反弹shell
		可令执行确测头例,反理shell xray基础使用、爬虫扫描、被动扫描
	web扫描器	awvs联动xray、burpsuite联动xray、rad联动xray、xray脚本编写
3"	Eige .	goby使用、nuclei使用
	弱口令	弱口令分类与字典 网站弱口令爆破
	99 🗆 🗸	常见服务弱口令爆破
		未授权访问概述
	未授权访问	redis未授权访问、redis利用写webshell、写ssh公钥、写计划任务、主从复制
		hadoop未授权访问 weblogic简介
	weblogic	weblogic河介 weblogic环境搭建
		weblogic历史漏洞发现与利用
		jboss简介
	j bos s	jboss环境搭建
常见漏洞		jboss历史漏洞发现与利用 struts2简介
	struts2	struts2环境搭建
	337	struts2历史漏洞发现与利用
	thinkphp	thinkphp简介
		thinkphp命令执行漏洞利用 fastjson简介、json认识
	fastjson	fastjson反序列化利用
		JNDI注入+RMI LDAP
	shiro	shiro组件简介
		shi ro550、shi ro721漏洞原因、特征判断与漏洞利用 log4j2简介
	log4j2	log4j2洞/环境搭建、利用与修复
A OFF		metasploit安装、配置
	metasploit	metasploit模块使用
	motaspioit	msfvenom生成后门
	lis de la companya della companya de	meterpreter后渗透命令详解 viper安装与配置
	viper	viper基本使用 、viper运行模块

£ 13"		cobaltstrike简介、基本使用	初级
St. 1818	cobaltstrike	监听器详解、beacon分类及工作原理、beacon使用	中级
7.		ms f 与cs流量分析	中级
渗透测试框架		隧道转发代理隐藏流量	高级
	进阶-流量隐藏	域名+CDN上线隐藏IP	高级
		转发重定向 CS配置文件隐藏流量	高级 高级
		cobaltstrike扩展脚本	中级
	进阶-拓展应用	CS上线linux主机	中级
-//		CS联动MSF、MSF联动CS	高级
39-		powershell简介	初级
43, 00,	powershell渗透框架	powershell脚本执行策略	中级
Ola Sala	•	powershell加载器	中级
		powershell工具框架-powersploit、nishang 内网渗透简介	中级初级
1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	**	windows工作组环境简介	初级
112	内网信息收集	windows域环境简介	中级
		机器位置判断、机器角色判断、连通性判断	初级
		域环境搭建、域内主机及用户管理	中级
		Hash简介	中级
		LM-HASH、NTLM-HASH windows本地认证、windows网络认证、windows域认证kerberos协议	中级
	密码凭证获取	windows 本地以准、windows 內容以准、windows 以从证kerberos 协议 系统用户凭证获取与破解	高级 高级
		其他常见应用服务密码获取与解密	高级
56		域环境密码凭证获取与解密	高级
A Offi		socks代理简介	中级
41,30.	内网代理	socks代理多级内网渗透环境实战	中级
内网渗透	137373	ITTP代理	中级
\$ 1300 E		DNS隧道、ICMP隧道 windows、linux操作系统提权	高级
No. Williams		metasploit提权、cobaltstrike提权	初级 中级
7	提权	域提权	中级
7		mysql提权、mssql提权	中级
		内网横向移动	中级
		IPC、Schtasks、WMIC、WinRM	中级
	横行移动	psexec、wniexec	中级
		pth哈希传递 域横向移动	高级 高级
1/2		windows、linux操作系统权限维持	中级
4	权限维持	域权限维持	高级
44) " 00,		ptf	高级
	痕迹清除	windows、linux日志、历史记录清除	初级
A THE	/2.	免杀概念	初级
ald.	127	免杀测试环境 常见杀毒软件检测技术	中级中级
<b>免杀</b>	免杀基础篇	吊见示母软件恒测技术 shellcode简介	高级
		shellcode加载器	高级
		常见免杀方式、免杀工具	高级
		shellcode混淆免杀	高级
	免杀进阶篇	shellcode分离免杀	高级
		C++加载shellcode	高级
		python加载shellcode 渗透测试基本流程	高级 初级
	渗透测试总结		初级初级
	INVENTION WARNET	渗透测试综合实战靶场讲解	高级
综合实战靶场	多级内网、域环境实战渗透靶场	W 4.20.	
165 1100	简历指导	B 180	
就业指导	简历制作	"Es Les	
N.	岗位内推		

HI WANTER TO THE STATE OF THE S

「大学   大学   大学   大学   大学   大学   大学   大学		A CALLED ON THE		HAD COL	46	A A Section of the Se
Linux操作系统而介	, di				The Day	
Linux操作系统	61	课程分类	课程大纲		1821 12	
Vinux操作系统	3		Linux系统简介		412	
Linux操作系统			VM虚拟机			
VIMSHERS         Virin编辑、保存、常见用法         初级           Linux服务及软件         远程连接组机、压缩包、Linux交装软件、Linux死场环境搭建         初级           Linux docker         docker变裂、docker基础使用         初级           PHP结别         PHP结果         有效           PHP结局         基本语光流 常量和变量、表达式运算符控制语句         初级           PHP结局数据         中级         中级           PHP结局数据         中级         中级           PHP结网域和操作         初级         初级           PHP结网域和操作         初级         初级           PHP结场或自数指库         初级         初级           PHP结场或自数指库         初级         初级           PHP结场或自数指库         初级         初级           PHP结局数据库         初级         初级           PHP结局对域支援库         初级         初级           PHP结局对域支援库         初级         初级           PHP结局对域支援库         初级         初级           PHP结局对域方域方面         初级         初级           PHP结局和操作         有级         有级           PHP结局和操作         有级         有效           PHP结局和操作         有效         有效           PHP结局和操作         有效         有效           PHP结局和操作         有效         有效           PHP结局和操作         有效         有效		Linux操作系统	Linux基础命令	命令行关机、重启		初级
Linux服务及软件         远程连接虚拟机、压缩包、Linux安装软件、Linux靶场环境搭建         初缀           Linux docker         docker姿装。docker基础使用         初级           PHP 基础         基本语法、常量和变量、表达式宣算符控制语句         初级           PHP面向对象         面向对象基础、类和对象         中级           PHP与Mysql数据库         如级         中级           PHP专Mysql数据库         初级         中级           PHP安全隐患         的方性包含问题         初级           PHP安全隐患         内内文件包含问题         初级           PHP安全隐患         内内工作包含问题         初级           PHP安全隐患         内的50m需要提和运行         初级           PHP东全隐患         内的50m需要提和运行         初级           PHP东全隐患         内的50m需要提和运行         初级           PHP安全隐患         内的50m需要提和运行         初级           PHP安全隐患         内的50m需要是和运行         初级           PHP安全隐患         内内50m需要是和运行         初级           Indiana         1avaScript 同分         初级           Indiana         1avaScript 可用         初级           Indiana         1avaScript 可用         初级           Indiana         1avaScript 可用         初级           Indiana         2xixixixix         初级           Indiana         2xixixixix         初级           Indiana         2xixixixx			VIM编辑界			
Linux docker					<b>不</b> 倍	
PHP 经础         PHP 全部、PHP 安装 对 全型 表达式运算符控制语句         初级 PHP 面缀 PHP 面侧对象 基础、类和对象 中级 面向对象基础、类和对象 中级 图形 可数 图形 图					I DUIH AL	
PHP基础         基本语法、常量和变量、表达式运算符控制语句         初级           PHP面向对象         的数         中级           PHP画向对象         中级         中级           PHP与Mysql数据库         初级         初级           php生的xss         初级           php中的xss         初级           php中的xss         初级           php生的xss         初级           php生的xss         初级           phpt生包含问题         初级           phpstorm定量应的和node;s         初级           ITML常用标签         初级           (SS样式表         初级           table标签和form表单         初级           JavaScript 面向介         初级           JavaScript 面介         初级           JavaScript 面介         初级           AvaScript 面介         初级           JavaScript 面介         初级           AvaScript 面介         <		PHP编程	Britax docker			
PHP高载         初缀           PHP面向对象         面向对象基础、类和对象         中级           面向对象基础、类和对象         有级           php 与Mysql数据库         初级           php 生物ysql数据库         初级           php 生物 数据         有级           php 生地方         有级           ph 5年         有级           ph 6年         有级           ph 7年         有级           ph 7年         有级           ph 7年         有级           ph 7年         有级			PHP基础			
PHP衛科         PHP衛列sql数据库         由內对象基础、类和对象         中级           PHP与Mysql数据库         初缀         初缀         初缀           PHP安全隐患         的应生接wscl数据库         初缀           PHP安全隐患         的级         初缀           PHP安全隐患         初缀         初缀           Dhrstorm发程包含问题         初缀           Dhrstorm发程包含问题         初缀           Dhrstorm发表和运行         初缀           IML常用标签         初缀           IML常用标签         初缀           Iable标签和form表单         初缀           JavaScript Iml         初缀           JavaScript Dmf         初缀           JavaScript DM         初缀           JavaScript DM         初缀           实践PoSrid来         初缀           网络开发实践         有级           网络开发实践         有级						
PHP·马mysql 数据库   初缀   初缀   内的连接mysql 数据库   初缀   内的连接mysql 数据库   初缀   内的连接mysql 数据库   初缀   内的中的yss   初缀   内的文件包含问题   初缀   内的文件包含问题   初缀   内的文件包含问题   初缀   内的storm安装和运行   初缀   内的storm定置的的和nodeis   初缀   内的storm定置的的和nodeis   初缀   内的storm定置的的和nodeis   初缀   日本公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公公			PHP面向对象			中级
Php安全隐患						初级
PHP安全隐患         向hp文件上传 向hp文件上传         初缀 初缀 向hp文件上传           开发环境安装         向hpstorm安装和运行 向hpstormc置向p和nodeis 前端语言基础         初缀 可缀 (SS件式表         初缀 有别级 日数 日本公Script 前介 日本公Script 前介         初级 日本公Script 前介 日本公Script 数据、对象、ison         初级 日本公Script 数据、对象、ison         初级 日本公Script 初级 日本公Script 数据、对象、ison         初级 日本公Script 数据、对象、ison         初级 日本公Script 初级 日本公Script 数据、对象、ison         初级 日本公Script 数据、对象、ison         初级 日本公Script 数据、对象、ison         初级 生数1-POST请求 等数2-Ajax请求         初级 等数3-Ajax请求         初级 等数3-Ajax请求         初级 等数3-Ajax请求         初级 等数3-Ajax请求         初级 等数3-Ajax请求         初级 等数3-Ajax请求         初级				php连接mysql数据库		初级
DhD文件上传   初級			PHP安全隐患	php中的xss		初级
开发环境安装     phpstorm安装和运行 phpstorm使置为pp和node; s     初级 初级 初级 (SS样式表 table标签和form表单     初级 初级 有效 有效 有效 有效 有效 有效 有效 有效 有效 有效 有效 有效 有效					<.	
Physiotring   置かり和nodeis   初後						
Phys tormic a physics and a			开发环境安装		4/4/5-	
前端语言基础				phpstorm配置php和nodejs	745	
Table标签和form表单   初缀			前端语言基础			
JavaScript	7.57				97.	
Figure						
JavaScript			JavaScript	JavaScript简介	7.	
Javabcript 数据、对象、Ison		网站开发				
实践1-POST请求     初级       实践2-A1ax请求     初级       网站开发实践     实践2-输出数据到页面     初级						
实践2-Ajax请求 初级 网站开发实践 实践3-输出数据到页面 初级						
网站开发实践 实践3-输出数据到页面 初级			m → + 11. 4> - d→ 114.			
大奴4-增加权证、大戏归尽			M站并及头政		-	
实践5-文件上传 初级						

WA-SA		
in the	蚁景网安渗透测试(红队方向)	学习服务
学习服务	1v1学习计划制定 班主任全程督学 讲师在线答疑 项目实战 各阶段考核测评 结业考核 就业指导 简历优化 就业帮内推服务 原创现金激励制度	

A A STEP OF THE ST