?????2025-05-14 09:28:28

???????

? ?

??

??(?45?)

1?????

?? ???????????????? ??????????? ?????? ?????????? ??????????? ???????? ????????? ??~

2?????????????

????????????? ??????????? ?????????????????????????? ??? ?


打工是不可能的
这辈子都不可能打工的
——窃·格瓦拉

??????????????????? ???????? ??????? ??????????? ?????????? ??????? ???? ???????????? ????????????? ???????? ??????????? ?????????? ?

??????????????????? ?????????????:????????????? ????? ????????????? ?

????????????? ????????????? ???????? ??????? ????????????? ?????????? ?????? ??????????? ?

??????????,????????????,??*???????,?????,????????????????????????? ?????????? ??????? ????????????? ???????????? ????????? ?

2.1???????

????????????? ????????????? ???????????????? ???????? ?????????? ????? ????????????? ????????? ???????? ????????????? ????????????? ?????????? ? ??????????????????? ?

??????????????????? ??????? ???????? ????????????????? ????????????????? ??????????????? ??????????????????????????????????????? ?

2.2?????

???????????? ??????? ???????????? ?????????? ????????????? ???????? ? ?????????? ????????????????? ????????? ????????????????? ???????? ????????? ????????? ?

白蚁网安网络安全之零基础学习渗透测试系列课程目录

渗透测试基础篇

章目	课程小节	教学内容
第一章：渗透测试的常见环境搭建	ASP	[illegible]
	JSP	Apache Or PHPstudy
	PHP	PHP环境
	Tomcat安装	Tomcat
	dvwa 漏洞演练平台安装及功能介绍	安装与介绍
	Linux Kali安装	kali
	环境搭建之JAVA/Python	环境搭建
	环境搭建整合之宝塔	宝塔安装
第二章：HTTP协议讲解	http协议的状态码及返回状态	状态码及返回状态有哪些
	常见的请求方式及消息	get、post、put的请求方式
	渗透中的作用	WAF和CDN[illegible]
第三章：常见Web后门木马的查杀方法	(1) ASP、PHP、JSP脚本后门手工及工具检测	手工及工具检测
	(2) webshell箱子后门	网页木马查杀
	(3) 中国菜刀后门检查	一句话木马查杀
	(4) shift/放大镜/等服务器后门木马查杀	后门木马查杀
	(5) 免杀远控/隐藏用户等后门木马检测	服务器木马查杀
	(6) 病毒分析引擎后门检测	病毒分析
第四章：渗透测试中的信息收集	(1) 网站持有者信息搜集	① 搜索引擎 ② 站内搜集 ③ 备案查询 ④ whois查询
	(2) 通过IDC搜集持有者信息	① 管理者账户 ② 营业执照信息检测
	(3) 网站子域名收集	① 搜索引擎 ② 分字爆破 ③ 其他方法
	(4) Google黑客语法的用法	技巧以及敏感信息
	(5) 目标开放服务探测	① 敏感服务介绍 ② 如何利用TCP/UDP端口探测 ③ 探测网段存活主机的操作系统
	(6) 目标所属网段探测	④ 开放的一些服务
	(7) 网站真实IP查找	① 邮件查找 ② cdn绕过 ③ 子域名真实IP ④ 域名不同解析检测真实IP
	(8) 漏洞服务探测脚本	① 探测网站端口 ② 可能产生漏洞的服务
	(9) 网站危险信息探测	① Phpinfo ② 敏感目录 ③ 备份文件泄露 ④ java反序列化

渗透测试漏洞原理篇

章目	课程小节
xss漏洞详细讲解及防御	(1) 反射型xss注入漏洞原理剖析
	(2) 储存型xss注入漏洞原理剖析
	(3) dom型xss注入漏洞原理剖析
	(4) xss注入漏洞如何优雅地绕过filter
	(5) xss注入漏洞利用及框架的使用
	(6) xss注入漏洞实例分析
csrf漏洞讲解及防御	(1) csrf漏洞的原理剖析
	(2) csrf漏洞的表单构造
	(3) csrf漏洞利用方法
sql注入漏洞讲解及防御	(1) sql注入原理
	(2) 常用数据库注入
	(3) sql注入之读写文件
	(4) sql注入万能密码注入
	(5) SQL注入之盲注
	(6) sql注入之执行命令
文件上传漏洞讲解及防御	(1) 任意文件上传漏洞
	(2) js文件上传过滤绕过
	(3) mine类型上传过滤绕过
	(4) 条件竞争上传过滤绕过
	(5) 内容验证上传过滤绕过
	(6) 服务器软件解析漏洞

章目	课程小节
命令执行漏洞讲解及防御	(1) 命令注入原理及常用命令
	(2) 命令注入绕过过滤
	(3) 命令注入其他姿势
	(4) 如何在代码中规避
文件包含漏洞讲解及防御	(1) 文件包含漏洞原理
	(2) 文件包含漏洞利用之远程文件包含
	(3) 文件包含漏洞利用之本地文件包含
	(4) 如何修复文件包含漏洞
	文件包含漏洞案例分析
ssrf漏洞讲解及防御	(1) ssrf漏洞原理剖析
	(2) ssrf漏洞与内网探测
	(3) ssrf与redis联动getshell的激情
业务逻辑漏洞讲解及防御	(1) 业务逻辑漏洞的任意密码修改
	(2) 如何绕过网站密码修改验证
	(3) 支付逻辑漏洞分析
	(4) 四个奇葩逻辑漏洞案例分析

渗透工具篇

章目	课程小节
Metasploit 渗透工具详解	(1) metasploit安装
	(2) metasploit框架介绍
	(3) metasploit更新
	(4) metasploit多模块介绍
	(5) metasploit与nmap及nessus的协作
	(6) metasploit实践渗透靶机
	(7) metasploit后门利用
	(8) metasploit的对安全引擎技术
	(9) metasploit提权技术及渗透测试
	(10) metasploit维持访问
Nmap工具使用技巧	(1) Nmap 安装
	(2) Nmap 的脚本介绍
	(3) 利用Nmap进行简单的扫描
	(4) Nmap渗透的多种方式扫描
	(5) Nmap 的信息刺探功能
	(6) Nmap与安全审计
kali	(1) Kali的美化工作
	(2) 常用信息搜集工具
	(3) 常用漏洞利用工具
	(4) 常用的局域网攻击工具
	(5) 其他实用工具

章目	课程小节
扫描器工具技巧	(1) Burpsuite自带的scanner模块
	(2) Awvs使用详解
	(3) Nessus 使用详解
	(4) Appscan 使用详解
	(5) Zap 使用详解
	(6) Nikto 使用详解
	(7) Jsky 使用详解
	Metasploit 实现扫描
抓包/协议分析程序使用技巧	(1) wireshark使用及xplico分析pcap包文件
	(2) Fidder简单使用
	(3) Brupsuite简介
	(4) Burpsuite安装及资源获取
	(5) Burpsuite代理设置
	(6) Burpsuite抓包https新闻及手机抓包方法
	(7) Burpsuite的Repeater模块详解
	(8) Burpsuite的Intruder模块详解
	(9) Burpsuite的Comparer模块详解
	(10) Burpsuite的Scanner模块详解
	(11) Burpsuite扩展插件
国产优秀工具讲解	
分享各类实用脚本	

总结篇

总结篇课程		课程目录
后台权限风险检查（上）	渗透测试常见错误理解纠正	上课方式：直播+录播+1对1问题解答
后台权限风险检查（中）	Windows本地权限提升漏洞	报名方式：联系[illegible]605221068
后台权限风险检查（下）	Linux本地权限提升漏洞	

蚁安零基础课程未完结（编程篇）

1、PHP编程基础篇	2、PHP代码审计篇	3、HTML基础+ClickJacking讲解	4、Python编程及安全脚本开发

??????????????????? ???????????????? ???????????? ??????? ??????? ?? ?????? ????????????????? ????2??? ?????????? ???????????? ???????????? ??? ???????? ????????????????? ????????????????? ?

3?????

?? ???????????? ????????????????? ???? ? ????????????????? ?

4?????

[???????????????? ????????? ???????? PDF???????????.pdf word???????????.doc ???????????]

????

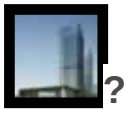
????

- ? ?????
- ?????1970-01-01 08:00:00
- ? ??????
- ? ? ???????????
- ? ??¥04.00 ?
- ? ? ????????????

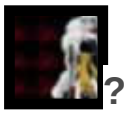
????

-
-
-

??60???



???



???

????

??????????

????,?????1003

??????????

[????????????]

[?????????????]

????

4940?

[? ?]

?????????

[??] | [????]