2023 年 Web 安全渗透+Kali 渗透高级工程师课程

新增 35 个渗透漏洞靶场+165 个渗透实战案例

学神IT教育

渗透安全

KALI渗透+WEB白帽子高级工程师

公司介绍

学神IT教育秉持只做“良心教育”的教学理念，多年来在国内IT在线教育一直名列前茅。讲师均具有企业多年实战经验，授课专业，并始终坚持“授人以鱼不如授人以渔”的培训理念。深入浅出的讲解每一个知识点，让每一个学员都能真正掌握核心实战技能，快速提高学员技术水平！

学神教学以实战经验为驱动，不仅能快速提升技术水平，更能让您的技术生涯步步高升。

想升职加薪、首选学神IT！

学神IT教育是腾讯课堂认证机构

资质与荣誉

redhat.

红帽官方授权认证合作伙伴
腾讯课堂认证培训机构

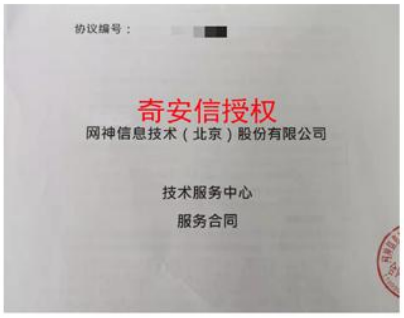
腾讯课堂
KE.QQ.COM

2015年腾讯课堂最受欢迎奖
2016年腾讯课堂最受影响力奖
连续9年腾讯课堂认证机构

腾讯课堂认证机构是由腾讯课堂发起的行业权威认证,对机构师资、服务、课程质量等进行综合评估后筛选出优质机构认证

网络运维类目认证机构
2017年腾讯课堂认证机构
2018年腾讯课堂认证机构
2020年腾讯课堂金牌机构
2021年腾讯课堂金牌薪选机构

资质与荣誉



与奇安信达成战略合作伙伴

与360达成战略合作伙伴

沃趣 WOQUTECH

杭州沃趣K8S云数据库公司
为我公司人才战略合作伙伴

与JumpServer公司达成合作

腾讯课堂薪选授权培训机构

2023 年 Web 安全渗透+Kali 渗透高级工程师课程

课程 1：零基础 Web 安全渗透工程师就业班

适合基础比较薄弱的学员，学完此课程后可达到就业水准。包括以下内容：

WireShark、FOFA、NMAP、ARL 灯塔系统、Metasploit、制作 Windows 木马、制作 Linux 木马、SQL 注入、PHP 开发、白帽子实战技巧、内网安全审计、暴力破解等 45 多个实战案例。

课程 2：Kali 渗透安全高级工程师进阶班

适合学完课程 1 或有渗透基础的学员，学完课程后可达到渗透高级工程师水准。包括以下内容：

XSS 跨站攻击、CSRF、SSRF、文件上传漏洞、扫描工具 AppScan、代码审计、XXE、Linux 应急响应、Linux 下手动查杀木马、隐藏进程踪迹、提权、劫持密码、免杀、绕过 WAF 防火墙、远程代码执行、内网安全审计、域渗透、SRC 挖漏洞、CTF、护网、红蓝对抗等 55 多个实战案例。

更多 VIP 课程专业问题，请您加老师微信为您解答。更有机会领取其他 VIP 学科的资料。详情如下：

2023 年课程更新以下内容：

1、全新课程内容更注重实战，从企业角度出发，带来全新的体验

2、课程内容整体更新

3、课程内容新增很多前沿技术

本课程包括 Kali、Centos7/8、Windows、Andriod 4 大操作系统的渗透安全课程体系。此教材由校长 MK 和 Root 讲师，联手打造的渗透安全课程体系。此次课程更新，增加了 35 个渗透隐患靶场和 165 个渗透实战案例。具体如下：

新增 35 个渗透隐患靶场，如：利用 cookie 获取 admin 权限的原理；web 日志管理系统-通过备份文件解密站点管理员用户密码的审计方法；SQL 注射系统-获取站点用户信息并实现任意文件读取的原理；XSS 获取 admin 权限的原理；DVWA 安全审计测试靶场；sqli-labs 靶场；OWASP Juice Shop 靶场；给商店一个毁灭性的零星反馈的防御方法；成功兑换过期的活动优惠券的审计等靶场。

新增 165 个安全审计实战案例，如：使用 Shodan 搜索引擎进行搜索的方法；使用 msf 安全审计 Win10 并进行远程关机的防御方法；使用 msf 扫描靶机上 mysql 服务的空密码的审计；使用 Windows 客户端安全审计获取电脑 shell 的原理；Linux 无文件恶意程序的审计；使用脚本来进行自动创建恶意程序的原理；窃取用户 Cookie 信息保存到远程服务器的防御方法；反射型 XSS 隐患对用户浏览器的安全审计；使用 LOIC 对新搭建的网站进行 DDOS 压力测试的防御方法；PHP 调用并执行 Linux 命令；离线破解 md5 值和 shadow 加密文件；使用蚁剑上传 webshell 恶意程序到网站的原理；使用 MITMf 实施中间人安全审计并利用 hook.js 脚本的审计方法；无线安全之通过 GPU（显卡）提升破解效率的原理；揭秘反弹 shell 对 360 等主流杀毒软件的免杀原理；免杀 D 盾一句话的审计；免杀 D 盾大马的审计；SQLI 联合查询类型过某狗 WAF 的原理；SQLI 盲注过某狗 WAF 的原理；域安全审计-横向安全审计获取域控最高权限的审计；使用 frp 搭建内网穿透服务器等案例;利用 HFish 蜜罐威胁感知捕获攻击数据;基于 IP 进行经纬度定位锁定攻击者;利用 HFish 蜜罐捕获攻击来源定位攻击者画像进行反制;利用 HFish 蜜罐收集攻击者账号密码监控失陷账号;基于 MySQL 蜜罐捕获敏感信息进行溯源反制;溯源反制获取 windows 机器登录的微信号信息与桌面截图;利用 HFish 蜜罐基于威胁检测规则检测潜在威胁;利用 HFish 蜜罐布置蜜饵或蜜标捕获攻击者。

VIP 学员独享教学特权：

1、直播+录播+笔记及源码+名师答疑+作业批改+阶段考核+项目答辩+全程就业跟踪服务的形式更适合高效学习

2、班主任定期跟进学习进度，回访学习情况，全程保驾护航

课程 1：零基础 Web 安全工程师就业班

(WEB、PHP、白帽子、SQL 注入、OWASP TOP 10、XSS、暴力破解、无线安全)

Kali 安全渗透+Web 安全工程师	
课程模块	课程要点

安装安全审计系统 Kali	Kali 是什么、为什么要安装 Kali、Kali 的发展史、Kali 的优势和特性 为什么要使用 Vmware 虚拟机软件，使用 VM 虚拟机安装 Kali 系统 安装 VM-Tools 实现物理机和 Kali 自由复制文件 配置 Kali 的 apt 使用国内源提升软件更新和安装速度 apt update ，apt upgrade 和 apt dist-upgrade 的区别
Kali 网络配置	本地网络配置，临时配置 IP 地址和永久配置 IP 地址，针对网卡桥接模式和 NAT 模式设置 IP 地址的注意事项和方法 配置 sshd 服务并使用 xshell 远程连接 Kali 系统
利用第三方服务对目标进行被动信息收集	被动信息收集概述，被动信息收集的特点，信息收集需要收集的信息，信息收集的用途、DNS 域名解析原理解析，什么是 DNS 服务器、域名解析记录详解 DNS 查询方式递归查询和迭代查询过程详解、使用 ping 命令将域名解析为 IP 地址、使用 nslookup 命令查看域名的解析 IP 地址、使用 dig 命令查询域名的详细解析记录获取更多信息 使用命令和在线工具查询域名的注册信息和备案信息 什么是子域名、挖掘子域名的重要性、使用 Layer 进行子域名挖掘 ARL 资产侦察灯塔系统搭建及使用、资产侦察灯塔系统升级 使用资产检索 FOFA 搜索引擎收集信息，FOFA 介绍、FOFA 基础语法、实战-FOFA 根据地区搜索、实战-FOFA 通过 icon 图标搜索资产、实战-FOFA 通过 JavaScript 文件查询、实战-通过使用 FOFA 规则列表搜索 CMS 资产 Google 搜索引擎常用搜索语法详解，利用漏洞库查询漏洞信息
主动信息收集	主动信息收集的原理、主动信息收集的特点、发现目标主机的过程 OSI 七层模型和 TCP/IP 五层模型详解 基于 ping 命令、arping 命令、netdiscover 命令、fping 命令的探测 TCP 三次握手和四次挥手原理及抓包过程详解 基于 Nmap 的扫描方式，使用 nmap 进行半连接扫描和全连接扫描 SYN 洪水安全审计和 DDOS 安全审计及防御手段、通过优化系统参数缓解 DDOS、通过 iptables 封禁攻击者 ip 缓解 DDOS
WireShark 抓包及常用协议分析	什么是 WireShark？WireShark 的应用、使用 WireShark 快速分析数据包技巧 常见协议包：ARP 协议、ICMP 协议、UDP-DNS 协议、TCP/IP 协议、HTTP 协议、HTTPS 协议、FTP 协议抓包及分析 实战：WireShark 抓包及快速定位数据包技巧 实战：使用 WireShark 对常用协议抓包并分析原理 实战：WireShark 抓包解决服务器被黑上不了网
NMAP 高级使用技巧和隐患扫描审计	什么是 NMAP？NMAP 主要应用方向、NMAP 端口状态解析、NMAP 语法及示例演示 NMAP 高级使用技巧、图形界面 zenmap 的使用、NMAP 脚本使用 什么是 NESSUS，NESSUS 发展历史，如何下载 NESSUS NESSUS 的安装和配置，详细讲解安装过程中容易出现问题的地方

	配置 NESSUS 并使用 NESSUS 对 windows 主机进行弱点审计并导出报告 配置 NESSUS 并使用 NESSUS 对 Web 站点进行弱点审计并导出报告
Metasploit 安全审计框架的基本使用	Metasploit 安全审计框架介绍、Metasploit 版本介绍 Metasploit 体系框架分析和详解、六大模块详细讲解和分析 Metasploit payload 常用形式和应用方式详解，Metasploit 目录结构详解 Metasploitable2-Linux 靶机系统搭建过程详解、什么是 PostgreSQL? Metasploit 的启动方式介绍、Metasploit 常用命令介绍及使用方法详解 揭秘使用 Metasploit 进行安全审计的原理 实战：使用 msf 安全审计 Win10 并进行远程执行命令的原理 实战：使用 msf 扫描靶机上 mysql 服务的空密码的审计
Metasploit 安全审计之信息收集	基于 tcp 协议收集主机信息 使用 Metasploit 中的 nmap 和 arp_sweep 收集主机信息、使用半连接方式扫描 TCP 端口、使用 auxiliary /sniffer 下的 psnuffle 模块进行密码嗅探的审计 基于 SNMP 协议收集主机信息 基于 SMB 协议收集信息，使用 smb_version 基于 SMB 协议扫描版本号、使用 smb_enumshares 基于 SMB 协议扫描共享文件的原理、使用 smb_lookupsid 扫描系统用户信息的原理 基于 SSH 协议收集信息，查看 SSH 服务的版本信息的原理、对 SSH 暴力破解的审计 基于 FTP 协议收集信息，查看 ftp 服务的版本信息的原理、ftp 匿名登录扫描的原理、ftp 暴力破解的审计
使用 windows 和 linux 客户端进行渗透的审计	什么是客户端安全审计，客户端安全审计的原理，客户端安全审计的技巧详解 揭秘生成恶意程序的原理 实战-注册机捆绑恶意程序上线 MSF 实战-WinRAR 捆绑恶意程序并自动上线 MSF 实战：揭秘通过制作 deb 软件包来触发恶意程序的审计方法
thinkphp rce-log4j2-宏感染-安卓客户端进行安全审计的原理和防御方法	Vulhub 靶场环境搭建 实战-thinkphp 5.0.23 rce 隐患复现 实战- log4j2 隐患复现 实战-利用宏感染 word 文档获取 shell 的审计方法 安卓客户端安全审计的原理及防御方法
揭秘 Metasploit 安全审计测试之制作隐藏恶意程序的原理	隐藏恶意程序的原理 实战-利用永恒之黑隐患对 win10 进行安全审计 创建一个新用户来远程连接 win10 桌面的审计方法 关闭主机防护策略并开启恶意程序的防御方法 实战：Linux 无文件恶意程序的审计方法 使用 msfvenom 生成恶意程序并结合动态库劫持创建无文件恶意程序并获取 Linux 系统的 Shell 的审计方法

	实战：使用脚本来进行自动创建恶意程序的审计方法 实现对恶意程序的持久性访问和权限维持的审计方法
Frp 内网穿透服务器在安全审计中的应用	局域网主机上网原理，实战-在内网发布服务使之可在公网访问，使用 frp 搭建内网穿透服务器，实战-kali 配置 MSF 接收来自公网的 shell 的审计，实战-跨网段获取内网 shell 的审计方法，实战：内网穿透-二级代理
SQLI 原理和 sqli-labs 实验环境搭建	通过 Web 应用的工作原理讲解 SQLI 产生的原因 什么是 SQLI？通过 SQL 语句拆分和组合深入讲解 SQLI 的原理 SQLI 的分类，布尔类型、联合查询类型、延时类型、报错类型，搭建 LAMP 环境，安装 sqli-labs 学习环境，安装浏览器插件 hackbar 方便进行 SQLI 审计，结合 SQLI-LABS 靶场讲解如何探测 SQLI 点发现 SQLI 隐患并判断字段数量和字段显示位置的审计方法 常见手动 SQLI 的闭合方式讲解，如何判断使用哪种闭合方式
联合查询-盲注-读写文件-报错类型 SQLI 审计	什么是 UNION 联合查询？UNION 联合查询的使用方法详解 使用 UNION 联合查询在 SQLI 中暴出字段的显示位置的审计方法 MYSQL 数据库常用函数讲解，SQLI-盲注，盲注的原理和分类，什么是盲注，为什么要使用盲注？盲注的分类，基于布尔的盲注和基于时间的盲注，盲注的逻辑关系详解盲注的流程、进行盲注的方法详解，通过实例讲解基于布尔的盲注的过程和原理，通过实例讲解基于时间的盲注的过程和原理
使用 burpsuite 进行 SQLI 审计	使用 Burpsuite 进行 POST 方式的 SQLI 审计、POST 方式的盲注审计 POST 方式的布尔型盲注审计、POST 方式的时间盲注审计、HTTP 头的 SQLI 方式审计，HTTP 头 SQLI 原理审计、通过对 XML 文档进行查询和修改函数的讲解并了解 HTTP 头 SQLI 的原理、HTTP User-Agent SQLI 审计、HTTP Referer SQLI 审计、Cookie SQLI 审计
SQLI 的基本防御手段和绕过技术的审计方法	SQLI 的绕过技术审计 通过大小写绕过对不区分大小写关键字的过滤进行 SQLI 审计 通过闭合绕过对注释的过滤进行 SQLI 审计 使用逻辑运算绕过对注释的过滤进行 SQLI 审计 使用双写绕过不区分大小写关键字的过滤进行 SQLI 审计 使用等价关键字绕过对关键字的过滤进行 SQLI 审计 使用空格编码绕过对空格的过滤进行 SQLI 审计 使用双写绕过对关键字的过滤进行 SQLI 审计 使用注释绕过对关键字的过滤进行 SQLI 审计 使用盲注绕过对关键字的过滤进行 SQLI 审计 GBK 编码使用 MySQL 宽字符绕过对特殊字符转义进行 SQLI 审计 使用 Base64 编码对注入语句进行编码绕过进行 SQLI 审计 通过二次 SQLI 修改其他用户密码的审计方法 针对 SQLI 如何进行有效的防御，防止 SQLI 的发生详解
使用 SQLMAP 自动化探测	SQLMAP 介绍，SQLMAP 支持的 SQLI 类型

SQLI 的审计	基于布尔的盲注检测、基于时间的盲注检测、基于错误的检测、基于 union 联合查询的检测、基于堆叠查询的检测、SQLMAP 常用探测方式，探测单个目标、探测多个目标、从文件加载 HTTP 请求进行探测、从 burpsuite 日志记录中进行探测、检测 SQLI 隐患存在的技术类型、枚举数据库信息的原理、SQLMAP 请求参数的设置及 SQLMAP 常用参数优化

课程 2：Kali 安全高级工程师进阶班

（CTF、靶场、Linux 渗透、护网、SRC 挖漏洞、红蓝对抗、内网安全审计）

Kali 安全审计+Web 白帽子高级工程师	
课程模块	课程要点
XSS 隐患的安全审计方法	什么是 XSS 隐患，XSS 隐患介绍 反射型、存储型、DOM 型 XSS 隐患利用的原理及详解 XSS 隐患利用原理及 DVWA 靶机的搭建 实战：窃取用户 Cookie 信息保存到远程服务器的审计方法
XSS 隐患的应用方式的审计	实战：反射型 XSS 隐患对用户浏览器的安全审计方法 修改页面链接的原理、构建反射型 XSS 隐患的审计、使用 beef 对用户浏览器的安全审计方法、beef 模块的使用 实战：持久型 XSS 窃取用户信息的审计 使用 setoolkit 克隆站点并获取账号和密码的审计 使用存储型 XSS 进行页面跳转的原理
XSS Challenges 闯关讲解 HTML 中的利用位置	XSS challenges 闯关游戏环境准备，了解 XSS challenges 闯关游戏的模式 XSS challenges 介绍，关闭 Google 浏览器 XSS-Auditor 防护功能 配置 burpsuite 加载证书用于截断 https 协议、Kali chromium 浏览器配置证书、Windows chrome 浏览器配置证书 手动进行 XSS 隐患审计 无过滤的 XSS 隐患审计，使用闭合标签方式进行反射型 XSS 隐患审计 属性中的 XSS 隐患审计，使用闭合 input 标签方式进行 XSS 隐患审计、在 input 标签属性中使用事件进行审计 选择列表中的 XSS 隐患审计，绕过过滤和转义通过 burpsuite 截断进行 XSS 隐患审计 利用隐藏域进行 XSS 审计，使用 burpsuite 截断数据包对隐藏域进行 XSS 隐患审计
XSS Challenges 绕过防护策略进行 XSS 隐患审计	XSS Challenges 闯关游戏进阶探测 XSS 隐患审计 绕过文本框输入长度限制进行 XSS 隐患原理及审计 html 事件中常见的鼠标事件介绍，并使用事件处理程序属性对限制输入<>进行 XSS 隐患审计

	绕过限制输入引号进行 XSS 隐患审计 JavaScript 伪协议，真伪协议讲解，利用 JavaScript 伪协议进行 XSS 隐患审计 UTF-7 编码安全审计，通过利用开发者工具结合 JavaScript 事件属性绕过关卡 通过双写 domain 关键字绕过正则匹配对 domain 关键字的过滤进行 XSS 隐患审计 通过对 XSS 隐患利用代码的编码和解码函数绕过对 domain 关键字的过滤进行 XSS 隐患审计 利用可以被浏览器忽略的空格字符编码对过滤 script 和 on 关键字进行 XSS 隐患审计 利用 IE 浏览器中使用反引号可以进行闭合的特性绕过防护策略进行 XSS 隐患审计 利用 IE 浏览器在 CSS 层叠样式表中对伪协议的支持特性进行 XSS 隐患审计 利用层叠样式表中的内联注释绕过对关键字的过滤进行 XSS 隐患审计
XSS 编码绕过审计以及自动化探测 XSS 隐患	XSS 渗透常用的编码，URL 编码、HTML 编码、JavaScript 编码、jsfuck 编码 URL 编码的由来及编码方式详解 HTML 实体编码的产生原因以及进制编码详解 JavaScript 编码，16 进制编码和 unicode 编码详解、jsfuck 编码详解及演示 使用编码绕过滤-进行 XSS 隐患审计，使用十六进制编码绕过过滤审计详解 字符转换成数字进制编码的方式详解 使用 unicode 编码绕过关键词过滤-进行 XSS 隐患审计 利用字典并使用 burpsuite 进行自动化测试 XSS 隐患 在 win7 上安装破解版 burpsuite，详解通过 burpsuite 进行代理抓包的原理 实战：在 win7 上使用破解版本 burpsuite 进行隐患审计
编码在 XSS 隐患中安全审计的应用	XSS 审计常用的编码 URL 编码、html 编码、javascript 编码、jsfuck 编码 使用编码绕过过滤-进行 XSS 隐患审计 XSS 编码技巧、浏览器解码顺序、字符串的分割、特殊的标签
CSRF 隐患审计方法	CSRF 原理、CSRF 隐患的定义，CSRF 与 XSS 的区别 基于 DVWA 的 low 级别进行 CSRF 隐患审计 通过代码审计分析 low 级别 CSRF 隐患的利用方式和原理 通过构造 URL 链接、验证 CSRF 隐患、构造恶意链接进行 CSRF 隐患审计 短连接介绍、如何生成短连接及短连接的使用场景详解 基于 DVWA 的 Medium 级别进行 CSRF 隐患审计 直接修改密码和通过其他页面提交请求的区别 通过抓取正常修改密码的 HTTP 请求和通过其他页面传入参数的请求对比 Referer 的区别、绕过 Referer 过滤的审计方法 基于 DVWA 的 High 级别进行 CSRF 隐患审计，测试 XSS(DOM)型 High 级别 通过 Ajax 获取 CSRF 页面内容并解析新的 token 进行 CSRF 隐患审计

	使用 CSRFTester 进行自动化探测 CSRF 隐患 CSRF 隐患自动化探测工具介绍，生成 POC 代码，对 CSRF 隐患进行验证
SSRF 服务器端请求隐患审计	SSRF 服务器端请求隐患简介 利用 SSRF 隐患实现端口扫描-任意文件读取的审计方法 SSRF 隐患利用 gopher 协议向内网发起 GET/POST 请求的审计方法 SSRF 隐患检测方法
基于文件上传隐患获得网站 shell 权限的审计方法	核心技术：蚁剑+一句话恶意程序 实战：基于 DVWA 的 low 级别文件上传隐患的审计方法 文件上传隐患简介、文件上传代码审计、Webshell 介绍、使用蚁剑进行连接一句话恶意程序获取 Webshell 权限的审计 实战：基于 DVWA 的 Medium 级别文件上传隐患的审计方法 截取上传文件的 HTTP 请求进行修改并进行重放的审计 实战：基于 DVWA 的 High 级别文件上传隐患的审计方法 制作简单的图片恶意程序进行上传绕过的审计，结合文件包含隐患获取 Webshell 权限的审计
Web 隐患扫描工具 AppScan 和 AWVS 使用方法	什么是 APPScan？APPScan 的安装及破解过程详解 APPScan 配置扫描 Web 站点的步骤和方法详解 Web 扫描器扫描报告的解读 白盒测试、黑盒测试、灰盒测试 AWVS 安装部署、xray 安全配置、使用 xray 进行主动扫描 Burpsuite 配合 xray 进行被动扫描
OWASP 十大安全风险和隐患的原理解析	OWASP Top 10 是对网站最关键的安全风险和隐患 A1.失效的访问控制 A2.加密机制失效 A3.注入 A4.不安全的设计 A5.安全配置错误 A6.自带缺陷和过时的组件 A7.身份识别和身份验证错误 A8.软件和数据完整性故障 A9.安全日志和监控故障 A10.服务端请求伪造
代码审计- discuz 论坛系统重置隐患审计	discuz 隐患原理分析和详解，部署 LAMP 环境，快速搭建带有隐患的 discuz 论坛 使用 kali 下 BurpSuite 对 discuz 后台植入 php 恶意程序的审计方法 使用蚁剑上传 webshell 恶意程序到网站的审计方法 使用 Webshell 查看 mysql 数据库密码并对数据库进行安全审计的方法
利用 XXE 隐患进行任意文件	XXE 隐患简介-XML 语法-DTD 讲解，什么是 XXE 隐患，XXE 隐患产生的原因

读取的审计方法	XML 介绍及用途，什么是 XML？XML 基本数据结构，XML 和 HTML 对比 XML 语法规则，XML DTD 介绍，XML 注入产生的原理 XXE 隐患的危害，通过加载恶意外部文件，任意文件读取、命令执行、内网端口扫描、安全审计内网网站、XXE 隐患代码详解，分析 XXE 隐患利用的思路，通过读取通过 POST 方式提交的 XML 代码并利用 simplexml_load_string()函数进行 XXE 审计分析 通过靶机 PentesterLab 实现无回显文件读取的审计方法 XXE 隐患修补，通过升级 libxml 版本以及代码层防御防护 XXE 隐患利用
代码审计-PHP 反序列化隐患审计	PHP 序列化基础概念 反序列化隐患审计实例-ctf ThinkPHP 5.1.X 反序列化任意代码执行隐患审计
密码分析常见服务审计	pydictor 介绍，pydictor 的下载与安装 实战：使用 pydictor 生成自己的字典工具 实战：使用 hydra 工具在线对系统用户密码进行密码分析，使用 hydra 对 Windows 7 文件共享密码进行密码分析、使用 hydra 对 windows 7 远程桌面密码进行密码分析、使用 hydra 工具对 ssh 服务 root 用户密码进行密码分析 实战：使用 Medusa 工具在线进行密码分析，使用 Medusa 工具对 windows 文件共享密码进行密码分析、Medusa 工具对 linux root 用户登录密码进行密码分析、Medusa 对 Mysql root 用户登录密码进行密码分析 实战：图形化密码分析软件 xhydra 使用方法 离线对 md5 值和 shadow 加密文件进行密码分析
密码分析-对 Apache BASIC 认证进行密码分析的审计方法	实战：通过对 web 登录界面进行密码分析获得管理员权限的审计方法，后台登录页面源代码审计，使用 burpsuite 进行密码分析的审计方法，使用 burpsuite 对 web 登录密码的审计方法，配置 Apache 的基本认证 BasicAuthentication 实战-对 Apache BASIC 认证进行密码分析的审计方法
Linux 应急响应-溯源-系统日志排查	Linux 应急响应-溯源-系统日志排查 查看当前已经登录到系统的用户、查看所有用户最近一次登录、查看历史登录用户以及登录失败的用户、SSH 登录日志分析、查看系统历史命令、计划任务日志分析、检查系统用户、中间件日志分析、通过时间检查站点被黑客修改过的文件、检查服务器已经建立的网络连接 通过 GScan 工具自动排查后门 巧用 systemd-journald 服务分析系统日志 实战清理系统日志后使用 systemd-journald 分析日志
揭秘 Linux 下手动查杀恶意程序过程-使用 rootkit 隐藏踪迹的审计方法	模拟恶意程序病原体并让恶意程序自动运行的审计方法，让脚本自动执行的审计方法 如何排查所有文件有没有被修改或追加内容详解 使用 rpm 检查文件的完整性、查看命令有没有被修改、如何校对所有的命令和包详解

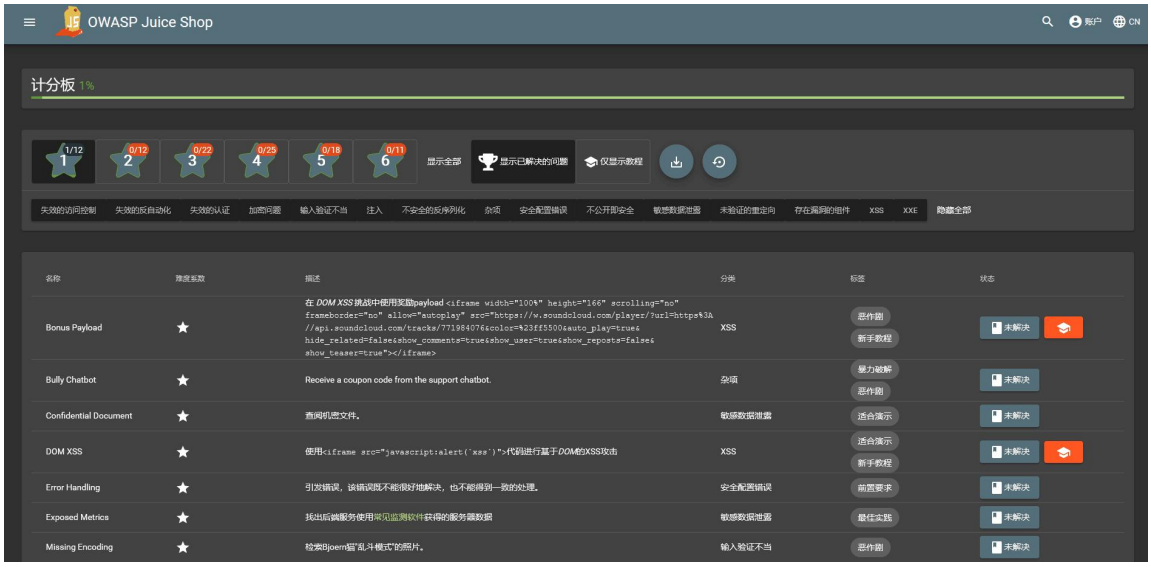
	Linux 权限维持脚本的原理解析、手工清理恶意程序 揭秘恶意程序父进程实时监控恶意程序的原理及防御方法 揭秘创建一个让 root 用户都删除不了的恶意程序的原理及防御方法 深入讲解如何不让恶意程序和外网数据主动通信 使用 rootkit 把恶意程序的父进程和恶意程序文件隐藏的审计方法 使用 rkhunter Rootkit 猎手来检查 rootkit
手工提升权限原理解析-Tripwire 检查文件	通过 CVE-2018-8120 隐患对 Windows 7 进行提升权限的审计方法 利用脏牛隐患（Dirty COW）在 CentOS 7 系统下进行提升权限的审计方法 如何防止利用脏牛隐患进行提升权限详解 自动窃取 root 密码并通过带外方式获取密码的审计，窃取 root 密码的原理解析及防御方法 使用 Tripwire 检查文件完整性，如何安装 Tripwire，配置 Tripwire 策略，验证 Tripwire 配置和检查系统，Tripwire 使用方法
无线安全	无线网络破解原理，无线网络协议标准、无线网卡的选择、无线加密方法 WPA-PSK 的认证过程，实战-破解 WPA 认证 wifi 的审计方法，虚拟机连接无线网卡、网卡初始化操作、查看网卡的详细支持信息、使用 airmon-ng 截取四步握手信息审计方法、离线破解密码的审计方法 实战-强制客户端重新认证-强制获取四步握手信息的审计方法 实战-隐藏 ESSID 破解的审计方法，通过 WPS 快速破解的审计方法 实战-通过 GPU（显卡）提升破解效率的审计方法 实战-绕过 MAC 地址绑定连接网络的审计方法
查找隐患并提交到补天 SRC 获得奖金	注册补天个人帐号，提交 SRC 流程，提交 SRC 需要注意的事项详解 企业入驻补天隐患平台，入驻流程详解 提交隐患-phpinfo 文件泄露系统信息 提交隐患-网站显示目录列表-mysql 备份数据泄露-网站安装目录信息泄露审计，提交隐患-SQLI 隐患审计
揭密反弹 shell 免杀的原理-PHP 远程代码执行隐患审计	实战-揭秘反弹 shell 对 360 等主流杀毒软件免杀的审计方法 主流免杀原理解析、分离免杀原理实战解析、内存免杀的原理审计、CS 免杀的原理解析 go 语言版本 shellcode 加载器免杀的原理审计 Apache Flink 任意 jar 包上传隐患审计 Flink 简介，什么是 Flink 简介，Apache Flink 环境搭建，生成反弹 shell jar 包、隐患修复方案详解 PHP-FPM 在 Nginx 特定配置下任意代码执行隐患审计 实战-PHP 远程代码执行隐患审计
揭秘 php 免杀马原理及防御方法-SQLI 过某狗 WAF 的审计方法	PHP 免杀马审计，D 盾简介、D 盾功能特性简介、D 盾的安装详解 免杀 D 盾一句话审计、免杀 D 盾大马审计 SQLI 过安全狗的审计方法，环境的搭建、安全狗的安装、sqli-labs 靶机的安装

	实战-SQLI 联合查询类型过某狗 WAF 的审计方法 实战-SQLI 盲注过某狗 WAF 的审计方法
CTF 学习之路	CTF 是什么？赛事介绍、CTF 都有哪些题目分类？为什么打 CTF?如何得分？ CTF 比赛模式，CTF 解题模式、CTF 模式、CTF 闯关模式 CTF 靶场练习，赛事以及题目信息、靶场练习实战演练
红蓝对抗	什么是红蓝对抗，在军事领域和安全领域分别解读红蓝对抗 红蓝对抗的目的、红蓝对抗关注点，外网 web 安全、办公网安全、IDC 主机安全、DB 专项 红蓝对抗测试的方法，按专项测试、按点排期测试、报告撰写，隐患闭环、例行扫描、持续跟进，复盘测试 红蓝对抗注意事项，测试前提前报备、有可能会影响到业务的操作时候务必提前沟通、隐患的确认按照公司的规范制度制定、隐患和业务沟通确认后再发工单修复、隐患闭环 护网行动应急响应概述，快速识别安全事件，快速分析与侦查
实战-内网安全审计之域渗透的审计方法	内网安全审计域基础知识详解，域安全审计环境准备和搭建 利用 weblogic 隐患并 getshell 的审计方法，利用 CVE-2019-2725 获得 shell 的审计方法 域安全审计-横向安全审计获取域控最高权限的审计方法，Cobalt Strike 简介，Cobalt Strike 部署 反弹 SYSTEM 权限的 shell 给 cs 服务的审计方法，明文读取密码的审计方法 域信息收集，通过凭证连接域控反弹域控 shell 的审计方法
渗透测试专用靶场	
Metasploitable-WEB 安全审计专用靶场  DVWA 安全审计演练系统	

加学神 IT 教育 净净老师 领课程资料 QQ：3367203381 官方 QQ 群：313034072

学神 Kali 安全课程新增 35 个安全审计隐患审计实战靶场

实战-OWASP Juice Shop 靶场挑战 OWASP TOP 10 风险隐患审计



实战-使用 Kali 多种安全审计工具渗透大型网站提交隐患并获得奖金

扩展课程-安全审计项目实战-录播课	
计算机取证	计算机取证概述 内存取证 使用 Volatility 对内存镜像进行分析 硬盘取证 使用 Autopsy 进行磁盘镜像分析 取证的难点
网络安全利用 ARP 欺骗实现中间人安全审计的审计方法	ARP 协议 ARP 工作原理 中间人安全审计原理 ARP 欺骗实现中间人的审计方法 利用中间人安全审计进行密码嗅探的审计方法
网络安全 DNS 污染原理及审计方法	DNS 原理 揭秘 DNS 污染方法 实战：局域网 DNS 污染的审计方法
ARP+DNS 污染 PC 的原理及审计方法	实战：内网 ARP+DNS 污染 PC 的审计方法 实战：伪装 ip 地址进行多线程 SYN 安全审计的审计方法
嗅探与欺骗的原理及审计方法	MITM 中间人安全审计理论 使用 MITMf 实施中间人安全审计植入 hook.js 脚本的审计方法
无线安全审计	无线技术概念 破解 WiFi 密码的审计方法 无线安全审计
XSS+BeEF+MSF 污染 PC 的审计方法	XSS+BeEF+MSF 污染 PC 的审计方法 BeEF 浏览器安全审计平台

	反射型 XSS 和 BeEF 浏览器安全审计的审计方法 存储型 XSS 和 BeEF 浏览器安全审计的审计方法
防黑技术	实战：搭建蜜罐系统捕捉威胁操作的步骤 手动恶意程序查杀过程 防止 DDOS 压力测试 被黑后-抓虫小技巧-把恶意程序帐号找出来 实战：检查 rootkit 恶意程序
seay 代码审计	通读全文法 敏感函数参数回溯法 定向功能分析法 自动化白盒审计 代码调试 正则编码 自定义插件及规则

学神 IT 教育祝你早日成为：

Kali 安全渗透+Web 白帽子高级工程师