2023 年内网渗透安全高级工程师课程

学神IT教育

内网安全

域渗透安全工程师

公司介绍

学神IT教育“是国内IT在线教育高端领导品牌，讲师授课专业度均为国内顶尖水准，授课方式深入浅出，课程内容全部采用企业实战项目案例的教学方式为主，能够让处于零基础小白状态的学员毕业获得工作经验，也能够让职场新人迅速提升技术水平获得加薪机会，更可以让工作多年的一线工程师走向项目主管、技术总监、架构师岗位。因此无论你是小白找工作，还是职场新人加薪跳槽，或是老司机走向高管、创业只路，“学神IT教育”都是你不错的选择！

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

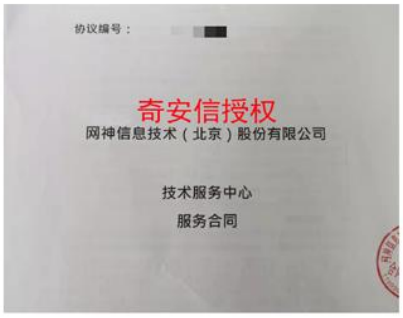
腾讯课堂
KE.QQ.COM

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

加学神 IT 教育官方 QQ 群:313034072 或 Root 老师 QQ:1260852266 领更多资料

2023 年内网渗透安全高级工程师课程

阶段一：内网渗透基础知识及原理

包括内容：工作组和域、域环境搭建、本地账户和活动目录账户、域组策略详解、域内权限详解

阶段二：内网渗透信息收集

包括内容：域中常见名词+服务主体名称、使用 Adfind 收集信息、使用 Ldapsearch 收集信息、使用 ADExplorer 收集信息、使用 Admod 收集信息、使用 BloodHound 收集信息等

阶段三：内网渗透常用攻击手法实战

包括内容：NTLM 协议详解、Kerberos 协议详解、域内用户名枚举、域内密码喷洒、票据操作、impacket 工具基础操作、AS-REP Roasting 攻击、Kerberoasting 攻击、Kerberos Bronze Bit 攻击、委派攻击、NTLM Relay 攻击、PTH 攻击（Hash 传递攻击）、Dsync 攻击

阶段四：内网渗透漏洞实战解析及防御

包括内容：MS14-068 权限提升漏洞、CVE-2019-1040 NTLM MIC 绕过漏洞、CVE-2020-1472 NetLogon 权限提升漏洞、Windows Print Spooler 权限提升漏洞、CVE-2022-26923 ADCS 权限提升漏洞、CVE-2021-42287 权限提升漏洞

阶段五：内网渗透权限维持

包括内容：域权限维持之 PTT 票据传递攻击、域权限维持之委派攻击、域权限维持之 DCShadow 攻击、域权限维持之 Skeleton Key 万能密码、域权限维持之 SID History 滥用、域权限维持之重置 DSRM 密码、域权限维持之 AdminSDHolder 滥用、域权限维持之 ACL 滥用、域权限维持之伪造域控、渗透密码搜集之 Hook PasswordChangeNotify、后渗透密码搜集之注入 SSP

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

第一阶段：内网渗透基础知识及原理	
课程模块	**课程要点**
工作组和域	1. AD、LDAP 2. X.500 标准定义的：DC、OU、CN、DN、RDN、UPN、容器 Container 3. FQDN 4. 对象 Object 与属性 Attribute 5. 工作组的特点、工作组的优缺点 6. 域的原理、域的结构(单域、域树、域林)、域的功能和特点

	7. 域功能级别和林功能级别 8. 工作组和域的区别 9. 单向信任、双向信任和快捷信任 10. 内部信任、外部信任和林信任 11. 域功能级别和林功能级别 12. 跨域资源访问和信任帐户
域环境搭建	1. 搭建 Windows Server 2008R2 域功能级别 2. 搭建 Windows Server 2012R2 域功能级别 3. 搭建额外域控制器 4. 搭建域树 5. 启用基于 SSL 的 LDAP(LDAPS)
本地账户和活动目录账户	1. 本地帐户 Local Accounts 的结束：administrator、Guest、 2. DefaultAccount、WDAGUtilityAccount 3. 活动目录帐户 Active Directory Accounts 之用户帐户 User Accounts 的介绍 4. 用户帐户 User Accounts 的操作 5. 服务帐户 Service Accounts 的介绍和操作 6. 机器帐户 Computer Accounts 的介绍和操作 7. 域目录分区 Domain Directory Partition 介绍 8. 配置目录分区 Configuration Directory Partition 介绍 9. 架构目录分区 Schema Directory Partition 的介绍 10. LDAP 中的类和继承 11. Schema Directory Partition 中的类和属性 12. 应用目录分区 Application Directory Partition 的介绍 13. 条目属性分析
域组策略详解	1. 组策略的功能 2. 组策略对象 GPO：组策略容器 GPC、组策略模板 GPT、默认 GPO 3. 策略设置与首选项设置的区别 4. 组策略的应用时机 5. 组策略的应用规则 6. 组策略的管理：新建、查看、编辑、删除组策略对象 7. 组策略的安全问题之组策略首选项 GPP 提权 8. 组策略的安全问题之滥用组策略委派属性 9. 组策略的安全问题之利用组策略创建定时任务
域内权限详解	1. 安全主体 Security Principals 2. 安全标识符 SID 3. Windows 访问控制模型：访问令牌(Access Token)和安全描述符(Security Descriptors) 4. 访问控制列表 ACL(Access Control Lists) 5. 访问控制条目 ACE(Access Control Entries)和 ACL 的判断流程 6. SDDL 安全描述符定义语言：ACE 的结构和 ACE 的解析 7. 域对象 ACL 的查看和修改：使用图形化、adfind 和 powershell 脚本进行查询和修改

第二阶段：内网渗透信息收集	
课程模块	**课程要点**
域中常见名词+服务主体名称	1. 域控制器 2. 用户信息 3. 计算机信息 4. 组信息 5. 组织单位（OU） 6. 权限和访问控制 7. 委派权限 8. 账户策略 9. GPO（组策略对象） 10. 域信任关系 11. 登录事件和审计 12. 服务主体名称（SPN） 13. SPN 的配置：基于主机的服务和可复制的服务 14. 注册 SPN：SPN 注册权限、将 SPN 注册在域帐户和机器帐户下 15. SPN 的查询和发现：setspn、impacket、PowerShellery、PowerShell-AD-Recon
使用 Adfind 收集信息	1. Adfind 的参数介绍：连接选项、过滤选项、显示选项和查看帮助 2. Adfind 的使用说明 3. Adfind 的使用示例：查询域信任关系、域控、机器相关、用户相关、组相关、委派相关等
使用 Ldapsearch 收集信息	1. Ldapsearch 工具的参数介绍：连接选项、过滤选项和显示选项 2. Ldapsearch 的使用示例：查询机器相关、用户相关、组相关、委派相关等
使用 ADExplorer 收集信息	1. ADExplorer 的连接、查询过滤 2. ADExplorer 增加删除修改属性和查看对象属性 3. 使用 ADExplorer 导出活动目录信息本地查看
使用 Admod 收集信息	1. Admod 的参数介绍：连接选项、过滤选项和修改动作 2. Adfind 的使用说明 3. 查询域信任关系、域控、机器相关、用户相关、组相关、委派相关等 4. 创建用户、创建 OU 组织单位、将用户移动到指定 OU、删除用户、重置用户密码、修改用户密码、修改域的 MAQ 为 0
使用 BloodHound 收集信息	1. 安装 Neo4j 数据库、运行 BloodHound 2. 活动目录信息收集 3. 导入数据 4. 数据库信息、节点信息、分析模块、查询模块的使用
第三阶段：内网渗透常用攻击手法实战	
课程模块	**课程要点**
NTLM 协议详解	1. NTLM 协议分析

	2. SSP 和 SSPI 的概念 3. LM Hash 加密算法 4. NTLM Hash 加密流程 5. Windows 系统存储的 NTLM Hash 6. 工作组环境下的 NTLM 认证流程 7. 域环境下的 NTLM 认证流程 8. NTLM V1 和 NTLM V2 的区别 9. LmCompatibilityLevel 10. NTLM 协议相关安全问题分析
Kerberos 协议详解	1. Kerberos 协议解析 2. PAC 特权属性证书介绍：PAC 结构、PAC 凭证信息、PAC 签名、KDC 验证 PAC、PAC 在 kerberos 中的优缺点 3. AS-REQ 请求包分析 4. AS-REP 回复包分析：TGT 认购权证、Logon Session Key 5. TGS-REQ 请求包分析 6. TGS-REP 回复包分析：ST 服务票据、Service Session Key 7. AP-REQ&AP-REP 双向认证 8. S4u2Self&S4u2Proxy 协议 9. Kerberos 协议的安全问题
域内用户名枚举	1. 域用户名枚举原理讲解 2. 域用户名枚举工具介绍及演示：Kerbrute、pyKerbrute、MSF 模块 3. 域用户名枚举抓包分析 4. 域用户名枚举攻击防御
域内密码喷洒	1. 域密码喷洒原理讲解 2. 域密码喷洒工具介绍及演示：Kerbrute、pyKerbrute 3. 域密码喷洒抓包分析 4. 域密码喷洒攻击防御
票据操作	1. 使用 Psloggedon 定位用户登录的主机演示 2. 使用 PVEFindADUser 定位用户登录的主机演示 3. 通过查询域控日志定位用户登录的主机 4. 通过不同工具查询定位域控：Adfind、nslookup、nltest 5. 通过不同工具查询域管理员和企业管理员：Adfind、ADExplorer 6. 使用不同方式查询所有域用户 7. 使用不同方式查询所有域主机 8. 使用黄金票据+SID History 进行跨域横向 9. 使用 inter-realm key+SID History 进行跨域横向 10. 利用非约束性委派进行跨域横向 11. 获得林根域后的操作 12. 域林横向攻击防御
impacket 工具基础操作	1. psexec.py 远程连接原理、条件和命令介绍 2. smbexec.py 远程连接原理、条件和命令介绍 3. wmiexec.py 远程连接条件和命令介绍 4. atexec.py 远程连接命令介绍 5. dcomexec.py 远程连接命令介绍

	6. smbclient.py 远程连接命令介绍 7. 使用 secretsdump.py 获取域内所有用户的 Hash 8. 使用 ticketer.py 生成黄金票据 9. 使用 getTGT.py 请求 TGT 票据 10. 使用 getST.py 请求 ST 服务票据 11. 使用 lookupsid.py 获取域的 SID 12. 使用 samrdump.py 枚举域内用户 13. 使用 addcomputer.py 增加机器账号 14. 使用 GetNPUsers.py 进行 AS-REP Roasting 攻击 15. 使用 GetUserSPNs.py 进行 Kerberoasting 攻击 16. 使用 ticketConverter.py 进行票据转换 17. 使用 addspn.py 进行新增、删除、查询 SPN 18. 使用 smbserver.py 创建 SMB 匿名共享 19. 使用 exchanger.py 获得 exchange 的邮箱信息 20. 使用 GetADUsers.py 获得域内所有用户信息
AS-REP Roasting 攻击	1. AS-REP Roasting 原理详解 2. AS-REP Roasting 攻击过程演示 3. AS-REP Roasting 抓包分析 4. AS-REP Roasting 攻击防御
Kerberoasting 攻击	1. Kerberoasting 原理讲解 2. Kerberoasting 攻击过程演示：SPN 的发现、服务票据的请求、导出服务票据、离线破解服务票据 3. Kerberoasting 抓包分析 4. Kerberoasting 攻击防御
Kerberos Bronze Bit 攻击	1. Kerberos Bronze Bit 漏洞背景和描述 2. Kerberos Bronze Bit 漏洞原理和影响版本介绍 3. Kerberos Bronze Bit 漏洞复现 4. Kerberos Bronze Bit 漏洞预防和修复
委派攻击	1. 域委派的作用场景解析 2. 非约束性委派详解 3. 仅使用 Kerberos(K)的约束性委派详解 4. 使用任何身份验证协议(N)的约束性委派详解 5. 约束性委派的流程、S4u2Self 和 S4u2Proxy 详解 6. 基于资源的约束性委派流程详解 7. 详解判断谁拥有配置基于资源的约束性委派的权限 8. 基于资源的约束性委派的优势详解 9. 实战-基于资源的约束性委派攻击 10. 讲解使用不同工具查询委派属性的账号：查询非约束委派的主机或服务账户、查询约束性委派的主机或服务账户、查询基于资源的约束性委派的主机或服务账户 11. 实战-非约束性委派攻击之诱使域管理员访问机器 12. 实战-非约束性委派攻击之结合打印机漏洞攻击 13. 使用不同工具演示约束性委派攻击 14. 对约束性委派攻击进行抓包分析

	15. 实战-基于资源的约束性委派攻击 16. 对基于资源的约束性委派攻击进行抓包分析 17. 域委派攻击防范措施
NTLM Relay 攻击	1. 详解 NTLM Relay 的原理和过程 2. 详解和演示如何使用 LLMNR&NBNS 攻击捕获 Net-NTLM Hash 3. 实战-使用打印机漏洞捕获 Net-NTLM Hash 4. 实战-使用 PetitPotam 捕获 Net-NTLM Hash 5. 实战-使用 desktop.ini 和 scf 文件捕获 Net-NTLM Hash 6. 实战-使用不同的 payload 出发浏览器捕获 Net-NTLM Hash 7. 实战-使用 Outlook 客户端捕获 Net-NTLM Hash 8. 实战-使用系统命令捕获 Net-NTLM Hash 9. 实战-使用 office 捕获 Net-NTLM Hash 10. 演示使用 PDF 捕获 Net-NTLM Hash 11. WPAD 详解并分析其流程 12. 实战-配合 LLMNR/NBNS 投毒使用 WPAD 捕获 Net-NTLM Hash 13. 实战-配合 DNS IPv6 投毒使用 WPAD 捕获 Net-NTLM Hash 14. 重放 Net-NTLM Hash Relay To SMB 15. 重放 Net-NTLM Hash Relay To HTTP 16. 重放 Net-NTLM Hash Relay To LDAP 17. 实战环境下 NTLM Relay 的利用 18. 实战-全补丁场景下利用 NTLM Relay 攻击接管全域 19. NTLM Relay 防御介绍
PTH 攻击（Hash 传递攻击)	1. 本地账号和域账号哈希传递区别：UAC(User Account Control)、FilterAdministratorToken、LocalAccountTokenFilterPolicy 2. 使用不同工具进行哈希碰撞：CrackMapExec、MSF 3. 使用不同工具利用哈希传递进行横向移动：mimikatz、impacket、MSF 4. 更新 KB2871997 补丁产生的影响："Protected Users"组的支持、"Restricted Admin RDP"模式远程客户端支持、"Pass The Hash"增强保护 5. PTH 哈希传递攻击防御
Dsync 攻击	1. DCSync 的工作原理介绍 2. 如何修改 DCSync ACL 3. 使用不同工具进行 DCSync 演示：impacket、mimikatz、PowerShell 脚本 4. 如何使用 DCSync 获取明文凭据 5. DCSync 防御与攻击检测
第四阶段：内网漏洞实战解析及防御	
MS14-068 权限提升漏洞	1. 漏洞背景 2. 漏洞原理 3. 漏洞复现 3.1 权限提升至域管理员 3.2 漏洞抓包分析 4. 漏洞预防和修复
CVE-2019-1040 NTLM	1. 漏洞背景

MIC 绕过漏洞	2. 漏洞原理 3. 漏洞完整利用链 3.1 触发目标 NTLM 请求 3.2 LDAP 签名绕过 3.3 攻击目标的选择 4. 漏洞影响版本 5. 漏洞复现 6. 漏洞抓包分析 6.1 连接 Exchange 服务器 6.2 触发 Print Spooler Bug 6.3 Exchange 向安全研究员发起 NTLM 认证 6.4 安全研究员将协商请求流量中继给域控 6.5 NTLMSSP_NEGOTIATE 消息中继 6.6 NTLMSSP_CHALLENGE 消息中继 6.7 NTLMSSP_AUTH 消息中继，认证成功 6.8 通过 LDAP 修改域 ACL 7. 漏洞预防和修复
CVE-2020-1472 **NetLogon 权限提升漏洞**	1. 漏洞背景 2. 漏洞原理 2.1 Netlogon 服务 2.2 Netlogon 认证流程 2.3 漏洞产生原因 2.4 绕过签名校验 3. 漏洞影响版本 4. 漏洞复现 4.1 Python 脚本复现 4.2 mimikatz 复现 4.3 恢复域控的机器用户哈希 5. 漏洞预防和修复
Windows Print Spooler **权限提升漏洞**	1. 漏洞背景 2. 漏洞原理 2.1 漏洞成因分析 2.2 漏洞利用分析 3. 漏洞影响版本 4. 漏洞利用 5. 漏洞预防和修复
CVE-2022-26923 ADCS **权限提升漏洞**	1. 漏洞背景 2. 基础知识 2.1 安装 Active Directory 证书服务 2.2 PKI 公钥基础设施 2.3 PKINIT Kerberos 认证 2.4 证书模板 2.5 证书注册、查看证书、导出证书 2.6 不同后缀的证书

	2.7 活动目录数据库中的 ADCS 3. ADCS 的安全问题 4. 漏洞预防和修复
CVE-2021-42287 权限提升漏洞	1. 漏洞背景 2. 漏洞原理 2.1 漏洞核心点 2.2 S4u2self 请求 PAC 的生成 2.3 跨域无PAC 的 TGS 请求 PAC 的生成 3. 漏洞利用流程 3.1 新建机器用户 3.2 修改机器账号的 saMAccountName 属性为域控 3.3 请求 TGT 认购权证 3.4 修改机器账号的 saMAccountName 属性为非域控 3.5 请求高权限的 ST 服务票据 3.6 导出域内用户哈希 4. 漏洞复现 5. 漏洞预防和修复
第五阶段：内网渗透权限维持	
域权限维持之 PTT 票据传递攻击	1. 黄金票据传递攻击和白银票据传递攻击解析 2. 实战-使用不同工具进行黄金票据攻击：impacket、mimikatz、CobaltStrike 3. 实战-使用不同工具进行白银票据攻击：impacket、mimikatz、CobaltStrike 4. 黄金票据和白银票据的联系和区别 5. 票据传递攻击防御
域权限维持之委派攻击	1. 使用委派打造变种黄金票据 2. 对利用的用户进行选择：已经存在的有 SPN 的域用户、自己创建的机器账号、自己创建的域用户然后赋予 SPN 3. 实战-利用委派打造变种黄金票据进行域权限维持
域权限维持之 DCShadow 攻击	1. DCShadow 攻击的原理 2. 实战-使用 DCShadow 攻击进行域权限维持 3. DCShadow 攻击防御详解
域权限维持之 Skeleton Key 万能密码	1. Skeleton Key 万能密码详解 2. 实战-使用 Skeleton Key 万能密码进行域权限维持 3. 实战-绕过 LSA 保护策略使用 Skeleton Key 万能密码进行域权限维持 4：Skeleton Key 攻击防御详解
域权限维持之 SID History 滥用	1. SID 和 SID History 详解 2. 实战-使用 SID History 攻击进行域权限维持 3. SID History 滥用检测和清除：使用 PowerShell 进行 SID History 滥用检测、使用 zBang 进行 SID History 滥用检测、SID History 属性的清除 4. SID History 滥用防御
域权限维持之重置 DSRM 密码	1. 目录服务还原模式 DSRM 详解 2. 实战-重置 DSRM 密码进行域权限维持

	3. 介绍 DSRM 攻击防御
域权限维持之 AdminSDHolder 滥用	1. AdminSDHolder、Protected Groups 和 Security Descriptor Propagator 详解 2. 实战-利用 AdminSDHolder 进行域权限维持 3. AdminSDHolder 滥用检测和防御详解
域权限维持之 ACL 滥用	1. 使用 ACL 滥用进行域权限维持详解 2. 实战-使用 User-Force-Change-Password 扩展权限进行域权限维持 3. 实战-使用 member 属性权限进行域权限维持 4. 实战-使用 msDS-AllowedToActOnBehalfOfOtherIdentity 属性权限权限进行域权限维持 5. 实战-使用 DCSync 权限进行域权限维持 6. 实战-使用 GenericAll 权限应用于域用户进行域权限维持 7. 实战-使用 GenericAll 权限应用于机器用户进行域权限维持 8. 实战-使用 GenericAll 权限应用于组进行域权限维持 9. 实战-使用 GenericAll 权限应用于域进行域权限维持 10. 实战-使用 GenericWrite 权限进行域权限维持 11. 实战-使用 WriteDACL 权限进行域权限维持 12. 实战-使用 WriteOwner 权限进行域权限维持
域权限维持之伪造域控	1. 使用伪造域控进行域权限维持的原理 2. 实战-使用伪造域控进行域权限维持 3. 伪造域控攻击防御
渗透密码搜集之 Hook PasswordChangeNotify	1. Hook PasswordChangeNotify 攻击进行密码收集解析 2. 实战-使用 Hook PasswordChangeNotify 攻击进行密码收集 3. Hook PasswordChangeNotify 攻击防御
后渗透密码搜集之注入 SSP	1. 详解 SSPI 和 SSP 2. 实战-使用 mimikatz 以两种方式注入伪造的 SSP：内存注入、注册表添加 3. SSP 注入防御

学神 IT 教育祝你早日成为：

内网渗透安全高级工程师