2020年，HACK学习文章精选

原创HACK学习 HACK学习呀
2020-12-31原文

实战渗透类

记一次VPN引发的内网突破
记一次详细的内网渗透过程
记一次后台漏洞挖掘渗透过程
记一次漏洞挖掘实战之木桶短板
记一次因“打码”不严的渗透测试
小程序渗透 | 对酒店房间自助售货机的支付漏洞挖掘
记一次逃逸Docker的渗透测试
记一次微信小程序渗透测试
Badusb 攻击之MacOSX系统实战
记一次内衣渗透测试
记一次失败的实战渗透

APP渗透｜看我如何在APP中getshell
记一次渗透测试从XSS到Getshell过程（详细到无语）
一次信息泄露引发的越权
记一次逻辑漏洞的挖掘
记一次渗透测试从XSS到Getshell过程（详细到无语）
记一次代码审计到申请CVE到过程
一次敏感信息泄露引发的逻辑漏洞挖掘

打击黑灰产类

记一次传销诈骗网站的渗透测试
记一次诈骗网站的渗透测试
记一次XSS闲鱼诈骗网站到主机上线再到信息收集的过程
渗透某非法约X软件
粉丝被裸聊勒索诈骗，我们花了2个小时黑进了骗子后台
当粉丝遇到裸聊诈骗，我们花了1天时间控制了诈骗犯的电脑
近期高发支付宝/京东理赔/快递类诈骗，我们花了3个小时控制了诈骗犯的电脑
一部手机失窃而揭露的窃取个人信息实现资金盗取的黑色产业链
揭秘支付宝暗雷的背后，如何防范此类诈骗
记一次渗透 ｜ 被骗4000花呗背后的骗局
记一次白嫖X站盒子App的渗透测试
揭秘运营商黑产 流量劫持技术剖析
网贷诈骗猖獗，技术打击黑产团伙全记录
机缘巧合之下拿下个发卡网还撸了把羊毛
一个邀请码引出来的故事
自己的服务器被抓鸡，看我如何反击
记一次对钓鱼网站的XFF头注入
记一次渗透棋牌APP实录
记一次对PUBG吃鸡外挂病毒的反制过程

记一次渗透某黑灰产平台的通用XXF头攻击漏洞
记一次对钓鱼网站的XFF头注入
实战 | BC杀猪盘渗透一条龙
看我如何拿下BC站的服务器
记一次虚拟币的渗透之旅
渗透某非法约X软件
记一次X情漫画的XSS盲打
[反诈骗] 入侵骗子电脑-揭秘冒充企业老板诈骗全过程
被骗之后，可以在网上追回钱吗?
科普 | 黑客真的可以追回赌博网站的钱吗?

知识整理类

XSS触发语句备忘
PWN学习指南
LDAP注入入门学习指南
实战 | Python 编写端口扫描器
渗透测试-Getshell总结
ThinkCMF缓存Getshell
Linux本地提权漏洞复现与检测思路

干货工具分享类

多款工具分享干货 | Cobalt Strike4.2Win+Mac破解版
独家 | 最全的Badusb资料集合<独家视频+代码>
应急响应相关内容知识积累 https:...
SRC挖掘经验分享 https://g...
渗透测试之个人常用高效爆破字典
红队中易被攻击的一些重点系统漏洞整理

Java SpringBoot
相关漏洞学习资料+基于实战沉淀下的各种弱密码字典
个人的隐私保护,查询方法,开源信息收集(OSINT)对抗指南
干货 | ATT&CK渗透测试手册
Windows 下的提权大合集
CrossC2的2.0版本
水坑攻击 | Flash钓鱼弹窗优化版
干货 | GitHUB安全搬运工
干货 | GitHUB安全搬运工 Ⅱ
干货 | GitHUB安全搬运工 Ⅲ
干货 | GitHUB安全搬运工 四

免杀类

免杀方法大集结
免杀 | 利用Python免杀CS Shellcode
干货 | 免杀技术学习路线图
实战中exe文件免杀
ShellCode生成框架
ShellCode注入原理
Office如何快速进行宏免杀
打造一款Socket型免杀无弹窗的shellcode
干货 | Shellcode免杀总结<一>
干货 | Shellcode免杀总结<二>
干货 | Shellcode免杀总结<三>

挖洞渗透思路技巧类

文件上传的一个骚操作(低权限+BypassAV)
App渗透测试流程和技巧

精华 | SQL注入万能Bypass技巧
内网渗透 | 获取远程主机保存的RDP凭据密码
逻辑漏洞 | 支付漏洞学习
干货 | 登录点测试的Tips
浅谈APP漏洞挖掘之逻辑漏洞
一个对指定网站的渗透思路
渗透技巧-Hadoop命令执行
Cobalt Strike 上线微信提醒
渗透小技巧 | sqlmap_dns注入配置方法
CS如何配置通过CDN上线
Weblogic CVE-2020-2551漏洞复现&CS实战利用
代码审计 | 利用思维导图快速读懂框架和理清思路
SRC逻辑漏洞挖掘详解以及思路和技巧
Chrome 80.X版本如何解密Cookies文件
基于社工的钓鱼研究
红队攻防之邮箱打点入口
红队攻防系列之花式鱼竿钓鱼篇
鱼叉攻击-炮轰马的制作
钓鱼攻击中文件的几种姿势
如何养成良好的渗透测试项目管理习惯
绕过卡巴进程保护的一些总结
关于站库分离渗透思路总结
干货 | Windows取证分析基础知识大全，赶快收藏！
干货 | 超详细的渗透测试思维导图
记录一次前端JS加密绕过 | 绕过前端解密的两种方法
干货 | 做一个全方面的信息安全导航站点
手把手教你如何成为一名黑客
黑客是如何黑进一家公司的

内网渗透类

内网渗透 | 记录一次简单的域渗透
内网渗透 | 手把手教你如何进行内网渗透
内网渗透 | 记一次域渗透实战
内网渗透 | 内网中的信息收集
内网渗透 | 常用的内网穿透工具使用
内网渗透 | NPS内网穿透工具的使用
内网渗透 | FRP代理工具详解
内网渗透 | 基于IPC的横向移动
一次简单的内网渗透靶场练习

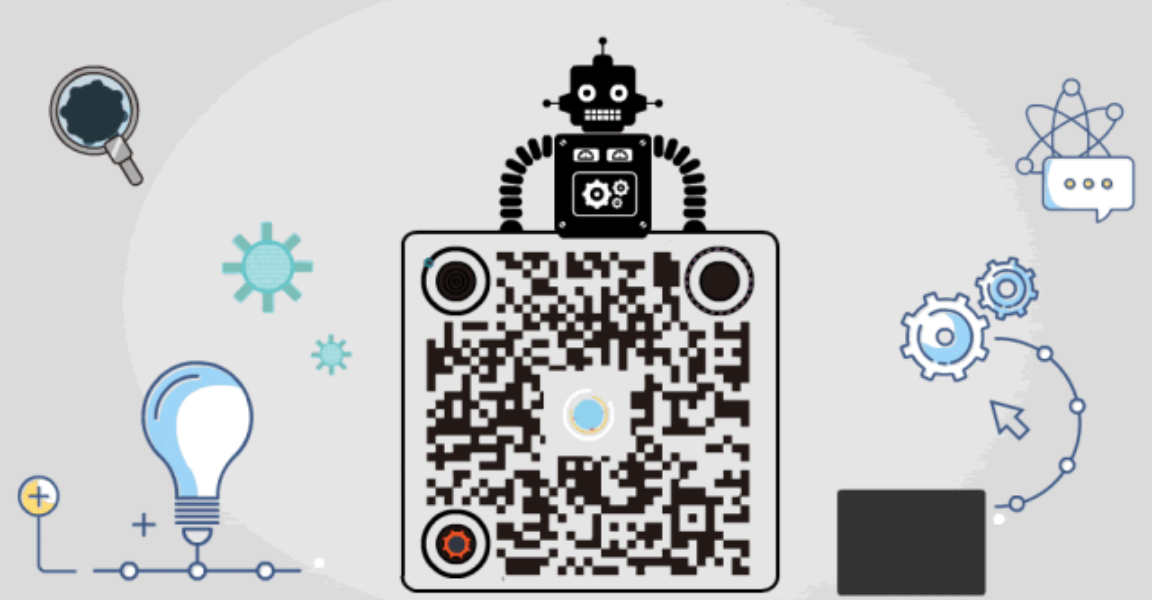
2020年
感谢各位小伙伴对HACK学习的支持和关注

2021年
我们将分享更多优质文章内容以及干货资源

提前祝各位小伙伴

元旦快乐

在新的一年里
没有日不下对站，没有完不成的KPI
新的一年，薪资翻翻



精选留言

用户设置不下载评论