2020-10-14

原创

我要当学霸！ 于 2020-10-17 09:49:33 发布 41 收藏

CTF黑客大赛

- **介绍，CTF需要的知识储备**
  –夺旗大赛–
  1.挖掘漏洞，利用漏洞进入对方的电脑，拿到关键文件
  2.xctf—>强网杯(中国的比赛),tctf，defcon
  ctf线上赛（web，二进制，杂项）---->
  ctf线下赛（web漏洞挖掘与利用10%，pwn漏洞与利用90%）
  能访问别人服务器：
  端口扫描：nmap：22,21,80,443,3306.。。。（踩点，如何进入对方机器，挖漏洞）0-65535 short
  3.知识储备
  –漏洞利用–二进制代码—木马 shellcode powershell
  python pwn tools
  web的机制 php js html：
  php有源码，jsp，javascriprt无源码
  web调试能力，代码审计（检查源码中的问题）、调试环境
  pwn漏洞挖掘：逆向分析， Linux系统知识
  漏洞利用脚本编写：远程触发漏洞
  流量分析能力：
- CTF比赛的神器
  kali系统（2018.02 kali）：有很多网络安全工具（nmap【端口扫描工具 139 443 514 】，searchsploit【漏洞查询】，metaspolit[攻击框架】、sqlmap sql注入的批量扫描、hydra ssh暴力破解、burpsuite）
  notepad++
  ue winhex
  wireshark
  pcap python lib
  文件监控武器
  权限检武器
  木马查杀武器
  批量攻击框架
  tly
  中国菜刀
- CTF的作用，[网络攻击、网络防御]
- CTF的经验
  web漏洞挖掘与利用
  ##基础划分：
  java web -->web漏洞挖掘，web服务器安全检测，web的代码审计，web常见的漏洞 web的补丁方法
  python ---->漏洞利用脚本设计
  PHPstudy–神器，【Mysql等所有环境的搭建、MySQL图形化管理界面、数据的导入导出】

PHPstudy+Xdebug(断点调试)+PHPstorm10
MySQL
Apache
Nginx
Python
常见题目类型：
Webshell：一句话木马 chmod
文件上传漏洞【客户端JavaScript检测（一般为检测文件拓展名：绕过方式：删除页面js检测代码，抓包工具修改包的内容，使用脚本进行攻击）、服务端MIME类型检测（检测Content-Type内容），】
文件包含漏洞 数据库攻击（sql注入） 反序列化攻击 XXE攻击
phpinfo

- 数据库攻击【直接拿flag】：flag在数据库 flag为本地文件
- 正则表达式