年复一年(18.8-19.7)

web 攻防&内网渗透 QQ 群：639882908

目　　录

一、CTF

1.1 CTF 相关：

CTF 社区：https://www.bugku.com/forum.php
CTF 在线工具网站：http://ctf.ssleye.com/
CTF-TOOLS：https://github.com/zardus/ctf-tools?files=1

1.2 WriteUp：

Vulnhub - Bob 靶机渗透攻略：https://xz.aliyun.com/t/2803
安洵杯 2018 官方 Writeup：https://xz.aliyun.com/t/3445
2018 护网杯 - pwn - writeup：https://www.codercto.com/a/31383.html
2018 CTF WriteUp 有 CTF 环境：https://www.freebuf.com/articles/web/185695.html
中国科学技术大学第五届信息安全大赛 CTF 题目：https://hack.lug.ustc.edu.cn/
UAF 实例—RHme3 CTF 的一道题：http://www.myh0st.cn/
实验吧-密码学解题思路及答案：http://m.bubuko.com/infodetail-2386870.html
Funny 的多媒体文件隐写题: http://url.cn/50NsyMR
图片隐写术：https://blog.csdn.net/binwalker/article/details/77716326
图片隐写术总结：https://blog.csdn.net/riba2534/article/details/70544076
CTF 密码学常见加解密总结: https://blog.csdn.net/qq_40836553/article/details/79383488
AWD 比赛总结：https://www.t00ls.net/tech.html
2018 西安工业大学第二届萌新线上赛密码学 WP：
https://blog.csdn.net/qq_42280544/article/details/82951044?utm_source=blogxgwz8
&#x 是什么编码以及转换方法：https://blog.csdn.net/jayxujia123/article/details/24580103
变量覆盖:https://www.cnblogs.com/test404/p/9779235.html
22 位四不像的 MD5 解密:http://www.hackdig.com/?01/hack-7873.htm
Md5（base64）加密与解密实战:
https://blog.csdn.net/jjjndk1314/article/details/80591814

二、常见漏洞

2.1 上传：

上传漏洞：https://www.cnblogs.com/shellr00t/p/6426945.html
文件上传-文件名长度绕过白名单限制：http://blog.51cto.com/eth10/2103563
HTTP - PUT 上传文件/Shell: https://www.cnblogs.com/kuoaidebb/p/4551764.html

2.2 注入：

注入——旁注：https://blog.csdn.net/Fly_hps/article/details/79508235
模板注入(SSTI)攻击(jinja2)：https://blog.csdn.net/qq_40827990/article/details/82940894
Access-SQL 手工注入实战:https://mp.weixin.qq.com/s/a-gSCJdSMBECid6GPMmo8A
Metinfo 利用 sql 注入快:getshell:https://nosec.org/home/detail/2324.html
代码审计 - dolphin.pro cms SQL 注入漏洞，Bypass 过滤规则:
https://www.freebuf.com/column/201787.html?from=groupmessage
移位溢注：告别依靠人品的偏移注入时代：https://www.t00ls.net/articles-38412.html
Access 数据库之偏移注入：https://www.cnblogs.com/xishaonian/p/6054320.html
MSSQL 注入提权,bypass 的一些总结:https://github.com/aleenzz/MSSQL_SQL_BYPASS_WIKI

2.3 逻辑漏洞：

逻辑漏洞挖掘：https://www.cnblogs.com/landuo11/p/7350445.html
应用程序逻辑错误总结：https://zhuanlan.zhihu.com/p/19728040
WEB 安全测试中常见逻辑漏洞解析：https://www.freebuf.com/vuls/112339.html

2.4 反序列化：

PHP 反序列化漏洞与 Webshell：https://www.t00ls.net/articles-44787.html
Java 反序列化漏洞从理解到实践：https://www.anquanke.com/post/id/86932
使用 burp 进行 java 反序列化攻击：https://www.anquanke.com/post/id/83571
java 反序列化漏洞 和 Java 序列化机制浅析：https://www.ddosi.com/b46/

2.5 Xss:

xss 漏洞之进制转换：https://max.book118.com/html/2016/0921/55299981.shtm
SRC 挖掘初探之随缘 XSS 挖掘:https://xz.aliyun.com/t/4625
使用 CSP 防止 XSS 攻击入门:https://blog.csdn.net/maquealone/article/details/79550144

2.6 Xxe:

Xxe 攻击：https://www.freebuf.com/articles/web/126788.html
Xxe 漏洞的学习与利用总结：https://www.cnblogs.com/r00tuser/p/7255939.html
XXE 漏洞的挖掘方法与防护 常见的漏洞类型：https://www.ddosi.com/b47/
XXE 漏洞学习从入门到放弃：https://www.jianshu.com/p/77f2181587a4
Web 安全-XXE 漏洞详解:
https://mp.weixin.qq.com/s?__biz=MzI1MDA4MTgwMw==&mid=2649086957&idx=1&sn=6f52b406cce248699acc520f880103fb&chksm=f196dc89c6e1559fc5e959a0b1a496379df75366401c4961cd56a520787e812b1fccb8676bb0&xtrack=1&scene=0&subscene=131&clicktime=1553949871&ascene=7&devicetype=android-25&version=2700033b&nettype=cmnet&abtest_cookie=AwABAAoACwATAAQAI5ceAFaZHgDFmR4A3JkeAAAA&lang=zh_CN&pass_ticket=i6huUAoEKUsD7NLRYNPJ0aHY4qW1wQSOVAbvWSqltm2BCL9eSszPsTIKCmjgKKoZ&wx_header=1
XXEinjector:https://github.com/enjoiz/XXEinjector

2.7 SSRF:

SSRF (Server Side Request Forgery) testing resources:https://github.com/cujanovic/SSRF-Testing

2.8 Csrf:

绕过 CSRF 的 referer 保护：http://www.cnblogs.com/zz0eyu/p/9789072.html

2.9 远程代码执行：

JMX RMI Exploit 远程代码执行实例：https://www.secpulse.com/archives/6203.html
从流量侧浅谈 WebLogic 远程代码执行漏洞：https://www.jianshu.com/p/f73b162c4649
Thinkphp5 框架缺陷导致远程命令执行：https://bbs.ichunqiu.com/thread-48687-1-1.html
SSRF Tips：http://blog.safebuff.com/2016/07/03/SSRF-Tips/
启明星辰 ADLab：ThinkPHP5 远程代码执行漏洞分析：https://mp.weixin.qq.com/s/XBcoT5ypV2cJ-Q09RS8JRA

2.10 任意下载：

任意文件查看与下载漏洞：https://www.jianshu.com/p/f4b06f59c4cb
任意文件下载漏洞基础和进阶 https://max.book118.com/html/2018/0627/8102114050001113.shtm

2.11 条件竞争：

一个有关竞争条件的攻击：https://blog.csdn.net/kylehit/article/details/5212412
测试 Web 应用程序中的竞争条件：https://www.freebuf.com/articles/network/107077.html

2.12 信息泄露：

信息泄露漏洞：https://blog.csdn.net/weixin_39997829/article/details/79836660

2.13 中间件：

Web 中间件常见漏洞总结：
https://mp.weixin.qq.com/s?__biz=MjM5NjA0NjgyMA==&mid=2651073796&idx=4&sn=852c7562962aa395e334072c6d64ddb7&chksm=bd1fbf8f8a683699c36af00b923ee0cb353905160706edad3121f50a61c9f593c0f8ad9ad34e&mpshare=1&scene=23&srcid=02236oHAeEtMHabEo8HLRGDt
Apache 曝出提权漏洞，可通过脚本升至 root 权限：https://nosec.org/home/detail/2446.html
Apache 官方漏洞集合：
https://httpd.apache.org/security/vulnerabilities_24.html?from=timeline&isappinstalled=0

2.14 其他：

OWASP top 10 漏洞的总结笔记：https://blog.csdn.net/SKI_12/article/details/69952026
常见高危漏洞及验证方法：http://blog.nsfocus.net/common-vulnerability-verify/
Web 应用的漏洞分类：https://wk.baidu.com/view/ba85246748d7c1c708a145e6.html
安全参考杂志(2013-2014 汇总)下载：https://www.waitalone.cn/security-reference-for-download.html
Web 业务安全测试—CORS 跨域资源共享漏洞:https://www.jianshu.com/p/68eed62233cc

三、博客社区

3.1 论坛社区：

先知社区：https://xz.aliyun.com/u/789?page=1

3.2 团队个人博客：

Arctic Shell 博客：https://www.cnblogs.com/
离别歌博客：https://www.leavesongs.com/
PyxYuYu-blog：https://github.com/PyxYuYu/MyBlog
JACK 个人博客：https://blog.barradell-johns.com/
VincentQB 的博客：https://blog.csdn.net/zwjzqqb/article/list/7
安全学习网站（Web 安全工程师路线）：https://www.jianshu.com/p/d667041e0698
博客--了解 Active Directory 的基础知识：https://blog.netwrix.com/
亮神博客:https://github.com/Micropoor/Micro8
Jai Minton: https://www.jaiminton.com/cheatsheet/DFIR/#
l3m0n:https://github.com/zMarch/Orc
雪碧:https://cn0xroot.com/

四、练习靶场

4.1 在线靶场：

网络信息安全攻防学习平台：http://hackinglab.cn/
XCTF 实训平台：http://oj.xctf.org.cn/
Vulhub 漏洞环境：https://vulhub.org/
Launch Your Project：https://www.vsplate.com/
墨者学院：https://www.mozhe.cn/bug
Web 安全在线练习平台：https://bbs.pediy.com/thread-218653.htm
分享一个好用的漏洞环境 Vulhub：https://www.freebuf.com/sectool/165062.html
蜜罐：https://github.com/paralax/awesome-honeypots/blob/master/README_CN.md
xss 靶场挑战之旅总结：https://blog.csdn.net/weixin_43027842/article/details/86897833
铸剑靶场 V2.0.1 :https://zhujian.zzyuncheng.com/
XSS:http://xss.fbisb.com/yx/level1.php?name=test

4.2 离线靶场：

BWVS：https://github.com/bugku/BWVS
BWAPP：https://sourceforge.net/projects/bwapp/files/bWAPP/
DVWA：http://www.dvwa.co.uk
WAVSEP：https://sourceforge.net/projects/wavsep/
Sqli-Labs：https://pan.baidu.com/s/1eRIB3Se
Webug 3.0：https://pan.baidu.com/s/1eRIB3Se
Upload-labs：https://github.com/c0ny1/upload-labs
Metasploitable：https://github.com/rapid7/metasploitable3
DVWA-WooYun：https://sourceforge.net/projects/dvwa-wooyun/
Web for Pentester：https://www.pentesterlab.com/exercises/web_for_pentester
OWASP Mutillidae：https://sourceforge.net/projects/mutillidae/

4.3 靶场讲解

zico 靶机实战过程:https://mp.weixin.qq.com/s/-92D5PP_jAPV1j3rwmj4HA
【HTB 系列】靶机 Access 的渗透测试详解:
https://mp.weixin.qq.com/s?__biz=MzU1NjgzOTAyMg==&mid=2247483909&idx=1&sn=b3d18ac0fce7233faa689e3880a26e9a&chksm=fc3fbb04cb483212464a96965f2c546dd4a788575d46a7296cdad4f5c7b14553ef45ce6dc2b7&scene=27&ascene=0&devicetype=android-25&version=2700033b&nettype=cmnet&abtest_cookie=BAABAAoACwASABMABQAjlx4AVpkeAMWZHgDXmR4A3JkeAAAA&lang=zh_CN&pass_ticket=4wteso8UCMOIWp6JunLjpgnH4M3lgDUCtIWdgTzQ4CxMHGJM8HrydTCNrHHchzYn&wx_header=1

五、漏洞复现

CVE-2018-8174 “双杀”0day 漏洞复现：https://www.freebuf.com/vuls/173727.html
2018 漏洞复现：https://pan.baidu.com/s/1PHhssMOHY_6KCMIR-P0-PQ
Struts2-057 漏洞从搭建到复现：https://mp.weixin.qq.com/s/L4LADYes1Mun44RdPMEeAQ
Thinkphp 框架漏洞复现：https://bbs.ichunqiu.com/thread-38284-1-1.html?from=kx4
Winrar 目录穿越漏洞复现：https://www.cnblogs.com/backlion/articles/10417985.html
从 WinRAR 中提取 19 年前的代码执行:
https://research.checkpoint.com/extracting-code-execution-from-winrar/
Jenkins RCE 概念验证：SECURITY-1266 / CVE-2019-1003000（脚本安全）：
https://github.com/adamyordan/cve-2019-1003000-jenkins-rce-poc
Thinkphp5.1 ~ 5.2 全版本远程代码执行漏洞：https://www.secpulse.com/archives/95248.html
Thinkphp5 框架变量覆盖导致远程代码执行：https://www.secpulse.com/archives/95191.html
WordPress 5.0.0 远程执行代码:
https://blog.ripstech.com/2019/wordpress-image-remote-code-execution/
致远 OA A8 poc 中的编码:https://bbs.pediy.com/thread-252286.htm
Ruby on Rails 路径穿越与任意文件读取漏洞分析 - 【CVE-2019-5418】: https://xz.aliyun.com/t/4448
Struts-S2-019 漏洞利用（含环境搭建、含 POC）:https://www.jianshu.com/p/c14ee451ddcd
Discuz!X 3.4 任意文件删除漏洞复现过程(附 python 脚本):
https://blog.csdn.net/qq_23936389/article/details/81255991
Weblogic 漏洞——从入门到放弃:
https://mp.weixin.qq.com/s?__biz=Mzg2NTA4OTI5NA==&mid=2247483778&idx=1&sn=b385adbdaf71b8e2757c893c4cda6866&chksm=ce5e23e3f929aaf509a959bee372fdc4969066df5dfd4998187ab64bbf1a0daa03de5b5eb948&mpshare=1&scene=2&srcid=&from=timeline&ascene=2&devicetype=android-25&version=2700033b&nettype=cmnet&abtest_cookie=BAABAAoACwASABMABQAjlx4AVpkeAMWZHgDXmR4A3JkeAAAA&lang=zh_CN&pass_ticket=zkjIrBw5%2BKlzY3j3EZaP7HdBYdjs8WgNBud4MZf%2FJqFWT7tWGSx3Ev7o6ROFievt&wx_header=1

六、渗透与权限维持

Powershell Wiki：https://www.peerlyst.com/posts/the-powershell-wiki-chiheb-chebbi
TorPCAP - Tor 网络取证：
https://www.netresec.com/?page=Blog&month=2018-12&post=TorPCAP---Tor-Network-Forensics
黑客在 Twitter 上披露新的未修补的 Windows 零日漏洞：
https://thehackernews.com/2018/12/windows-zero-day-exploit.html
Linux 权限维持之影子 SUID 的利用:https://xz.aliyun.com/t/4869

6.1 渗透测试技巧：

“撬锁”实战：绕过云锁提权某游戏私服：https://www.freebuf.com/articles/web/179761.html
绕过 cdn 获取网站的真实 ip：https://blog.csdn.net/qq_29277155/article/details/52463908
透过 F5 获取服务器真实内网 IP：https://threathunter.org/topic/5940c85d9c58e020408a79fe
MySQL 弱密码和 webshell（附可用于 php7 的菜刀）：https://www.jianshu.com/p/cd071dcfefe7
隐藏木马软件的三大黑客技术：http://m.sohu.com/a/190323884_478206
详解手机注册验证码操作思路与流程：https://blog.csdn.net/dunegao/article/details/78716391
利用 Thinkphp 5 缓存漏洞实现前台 Getshell：https://www.freebuf.com/articles/web/153286.html
网络黑白入侵技巧：https://www.jianshu.com/p/9590925dbd80
Cmd 下修改文件访问控制权限：https://www.kafan.cn/mip/edu/1582862.html
使用 PEloader 来加载 exp：https://evi1cg.me/page/3/
Linux 安全之 SSH 后门：https://www.jianshu.com/p/b394528051c6
嗅探、劫持 3389 端口、远程桌面、rdp 协议的一些经验技巧总结：
https://blog.csdn.net/zvall/article/details/50115499
内网安全防御实践（安全牛）：https://edu.aqniu.com/h5/index.html#/course/9416
网站入侵思路之渗透篇：
https://www.jianshu.com/p/e98a109616a6?utm_campaign=haruki&utm_content=note&utm_medium=reader_share&utm_source=qq
内网渗透 TIPS:https://github.com/Ridter/Intranet_Penetration_Tips
内网渗透知识基础及流程：
https://www.anquanke.com/post/id/170471?from=groupmessage&isappinstalled=0
Windows 单机权限维持 [wmi 事件]：https://www.cnblogs.com/klionsec/p/10297389.html
fwknop - 单包授权：
https://github.com/mrash/fwknop?sourceType=qq&from=singlemessage&wm=2468_90037&isappinstalled=0&featurecode=newtitle
Kali Linux 渗透测试:https://blog.csdn.net/Kevinhanser/article/details/78010013
内网渗透 TIPS:https://github.com/Ridter/Intranet_Penetration_Tips
高级组合技打造“完美” 捆绑后门:https://evi1cg.me/archives/chm_backdoor.html
对某网的一次渗透测试纪实:https://mp.weixin.qq.com/s/N-ghWPnMFz5IfWYlcIsMXg
windows 提权基本命令:https://blog.csdn.net/ws13129/article/details/89243703
sockscap+Bitvise Tunnelier 做内网渗透:https://blog.csdn.net/cnbird2008/article/details/6699830
从 404 到默认页面，通过.cshtml 拿到 webshell:
https://www.4hou.com/technology/4678.html?spm=5176.11156381.0.0.37c563f3vC9BpA
渗透测试实战之运气:
https://mp.weixin.qq.com/s?__biz=MzU2MjM4NDYxOQ==&mid=2247483963&idx=1&sn=7c94846e6886751594def5bcd24659fd&chksm=fc6b19bfcb1c90a93cd6a4036d865ea07ef0ca496f8fb38a1fa0a419c9d543c71fd742aeb35e&mpshare=1&scene=23&srcid=
[原创]利用 Browser 协议探测内网主机操作系统版本(无需端口无视防火墙)：
https://www.cnblogs.com/k8gege/p/10561336.html?sourceType=qq&from=singlemessage&wm=2468_90037&isappinstalled=0&featurecode=newtitle
[原创]记一次蔓灵花 APT 组织针对巴基斯坦定向攻击的样本分析:
https://bbs.pediy.com/thread-249319.htm

6.2 反弹 shell、端口转发：

Linux 下反弹 shell 方法：https://www.waitalone.cn/linux-shell-rebound-under-way.html
powershell 反弹 shell 常见方式：https://www.anquanke.com/post/id/99793
redis 未授权访问引起的反弹 shell 问题解析：https://cloud.tencent.com/developer/news/301606
redis 未授权访问反弹 shell：https://blog.csdn.net/sdb5858874/article/details/80822536
内网映射方案(lanproxy)：http://kekefund.com/2018/06/24/lanproxy/
内网端口转发穿透：http://www.zerokeeper.com/experience/network-port-forwarding-and-penetration.html
Kerberos 的黄金票据详解:https://www.cnblogs.com/backlion/p/8127868.html
利用 Windows one-liner 获取反向 Shell:
https://mp.weixin.qq.com/s/4T3KnWmkdpD2CZkAAvOJvA

6.3 其它知识点：

同时部署 WAF 和 CDN：https://help.aliyun.com/knowledge_detail/42200.html
对 CDN 的误区：http://www.rinige.com/index.php/archives/772/
php 下进行 mysql 参数化查询：https://blog.csdn.net/lpwmm/article/details/50733698
Poc 基础知识：https://poc.evalbug.com/chapter1/1.html
Linux 系统清除缓存【整理】：https://blog.csdn.net/qiuzhi__ke/article/details/70768544
大马小马的区别：http://www.cnhonkerarmy.com/thread-156156-1-1.html
面试必备之乐观锁与悲观锁：https://blog.csdn.net/qq_34337272/article/details/81072874
一套实用的渗透测试岗位面试题：https://zhuanlan.zhihu.com/p/25582026
IPC$、ADMIN$、C$、D$都是什么?如何关闭取消删除 Windows 默认共享：https://m.jb51.net/softjc/2124.html
linux 常见 backdoor 及排查技术：https://xz.aliyun.com/t/4090
黑客入侵应急分析手工排查：
https://www.cnblogs.com/shellr00t/p/6943796.html?utm_source=tuicool&utm_medium=referral
秘迹：https://m.mijisou.com/
在线病毒检测引擎：http://www.virscan.org/
云扫描病毒：http://www.scanvir.com/
威胁情报分析平台：https://x.threatbook.cn/partner
WebShell 检测引擎：https://scanner.baidu.com/
代理行动规则：https://github.com/PortSwigger/proxy-action-rules
研究个人编译 APT 恶意软件:https://github.com/sapphirex00/Threat-Hunting
高级威胁战术:https://www.cobaltstrike.com/training
SwitchHosts---快速切换主机：
https://github.com/oldj/SwitchHosts?sourceType=qq&from=singlemessage&wm=2468_90037&isappinstalled=0&featurecode=newtitle
Bypass AVs to Add Users：https://xz.aliyun.com/t/4078
思福迪堡垒机之绕过密码验证机制：http://vulsee.com/archives/vulsee_2019/0628_8035.html
安全岗位面经总结（持续维护）：https://www.shallowdream.cn/index.php/2018/07/06/50.html
微软最爽命令行工具发布！引诱开发者叛逃 Mac，开源六小时冲上 GitHub 第二:
https://mp.weixin.qq.com/s/YYzvi4FXwwCK7Hk-TwZ8kA
给 sqlmap 装上 chunk transfer 的辅助:https://mp.weixin.qq.com/s/9uoe1EQpQo9Qv24YIWr5gw
基于 VIM 漏洞 CVE-2019-12735 的 VIM 宏后门病毒详解：https://www.freebuf.com/vuls/205516.html
PC 傻瓜式安装黑苹果并打造成全能逆向工作站：https://www.freebuf.com/geek/149063.html
ShadowsocksR SSR 伪装网站访问方式 sspanel 混淆流量:https://www.svlik.com/384.html
警惕利用 Linux 预加载型恶意动态链接库的后门:https://www.freebuf.com/column/162604.html
awd 比赛中一些猥琐的思路总结：
https://mp.weixin.qq.com/s?__biz=MzI0NzcONTcwOQ==&mid=2247484467&idx=2&sn=53eae24537a10f523ad36480ae6f95ae&chksm=e9aa19f1dedd90e778c5232d245ed06a6c565b6653d09ec769dfd276add370c2ff5427

0826b4&xtrack=1&scene=0&subscene=131&clicktime=1552178994&ascene=7&devicetype=android-28&version=2700033b&nettype=3gnet&abtest_cookie=BAABAAoACwASABMABAAjlx4AWpkeAMyZHgDSmR4AAAA%3D&lang=zh_CN&pass_ticket=GCKp2zic%2BxYEEp6lB0DwM8mw0rYyEIh9LRA%2BYBHxIF%2BqIdpGcth9ePTuz9%2FZXKZ4&wx_header=1

2019 年 3 月安全更新审核：
https://www.zerodayinitiative.com/blog/2019/3/12/the-march-2019-security-update-review

几种常见远程访问策略详解：https://www.4hou.com/web/10270.html

红队与理论:https://paper.seebug.org/844/

红队基础建设:https://xz.aliyun.com/t/4509?secwiki&from=singlemessage&isappinstalled=0

七、学习资源与工具

7.1 墙外世界：

搬瓦工 VPS 优惠码：https://www.banwago.com/114.html
用 VPS 搭建网站的详细步骤：https://www.jianshu.com/p/2e3abc49464b
手把手教你搭建 shadowsocks 科学上网搭建 SS 翻墙：
https://www.textarea.com/shadowsocks/shoubashou-jiao-ni-dajian-shadowsocks-kexue-shangwang-dajian-ss-fanqiang-935/

7.2 电子书籍：

安全思维导图集合：https://github.com/SecWiki/sec-chart
程序员参考书集合：https://pan.baidu.com/s/1yVal4_teqv7diHrWy8RFA
PHP 编程：https://pan.baidu.com/s/1ZvUdonJ_h3EYTfHIbjoe6A
代码审计入门：http://www.cnblogs.com/Oran9e/p/7763751.html
墨者学院审计类通关指南：https://xz.aliyun.com/t/2821
Python win32 手册：https://download.csdn.net/download/jiaoxiaogu/3290313
Kali Linux Web 渗透测试手册(第二版) - 1.1 - 渗透测试环境搭建中文翻译：
https://www.cnblogs.com/7089fy/p/9992317.html
IT 畅销电子书：https://www.packtpub.com/
The-hacker-playbook3 最新版 PDF：
https://download.csdn.net/download/kevin2089764/10762932
[译] 渗透测试实战第三版(红队版)：
https://github.com/Snowming04/The-Hacker-Playbook-3-Translation?from=timeline&isappinstalled=0
《Linux Basics for Hackers》2019: https://github.com/OpenCyberTranslationProject/TP1
红队资料集锦:https://www.lshack.cn/772/
渗透 超全面的渗透资料:https://github.com/w1109790800/penetration
Weakpass 密码表:https://weakpass.com/
Python 速查字典:https://www.w3cschool.cn/python/dict
乌云 Drops 文章在线浏览:https://wooyun.js.org/
业余笔测试者指南和黑客工具：https://github.com/sundowndev/hacker-roadmap

7.3 资源网站：

WEB 安全扫盲公开课：https://www.bugbank.cn/live/websm
Web 安全学习资料：https://www.secfree.com/article/402.html
Oday 安全：http://www.0daysecurity.com/penetration-testing/enumeration.html
Kali Linux 渗透测试：https://mp.weixin.qq.com/s/8UcU7R803k3gcextswzGlQ
IT 资料搜寻网站:https://www.programcreek.com/java-api-examples/?action=search
风控预警平台: https://github.com/creditease-sec/insight

7.4 工具教程：

Metasploit 工具教程:

渗透框架下载：https://www.metasploit.com/
winx64 和 Linux 镜像下载：https://github.com/rapid7/metasploit-framework/wiki/Downloads-by-Version
学习 Kali Linux 各种破解教程、渗透测试、逆向工程 HackThisSite:https://github.com/tiancode/learn-hacking
Metasploit 入门教程渗透测试框架平台：https://bbs.ichunqiu.com/thread-40440-1-1.html
Meterpreter 免杀技巧分享：https://www.freebuf.com/sectool/118714.html
安全测试—利用 Burpsuite 密码爆破：https://blog.csdn.net/weixin_38948797/article/details/79111566
手把手教你如何用 MSF 进行后渗透测试：https://www.anquanke.com/post/id/164525
Meterpreter 免杀内网渗透：https://www.jianshu.com/p/0e7cf99098b9
【技术分享】使用 MSF 路由转发实现 MSF 框架的内网渗透：
https://www.360zhijia.com/360anquanke/279544.html?from=groupmessage
pentestbox 更新 msf 成功：https://www.icode9.com/content-4-96442.html

其他安全工具教程:

安全工具——御剑：https://www.cnblogs.com/anka9080/p/mlsm.html
Kali Linux 使用 Aircrack 破解 wifi 密码：http://topspeedsnail.com/kali-linux-crack-wifi-wpa/
密码破解等攻击手法：https://github.com/tiancode/learn-hacking/blob/master/README.md
黑客笔记|利用密码重置实现账号劫持：https://www.jianshu.com/p/012bc1ab1443
Kali Linux 下社工密码字典生成工具 Cupp 和 Cewl 教程：https://www.jianshu.com/p/74103727b9b7
fail2ban 防止暴力破解 nginx web 目录被黑客扫描：https://blog.csdn.net/dorisnzy/article/details/82926067
中国菜刀原理浅分析:http://www.ifuryst.com/archives/caidao.html
Burpsuite 神器常用功能使用方法总结：https://zhuanlan.zhihu.com/p/22288110
Burp Suite 中文乱码真正的解决方案：https://bbs.pediy.com/thread-248802.htm
史上最详[ZI]细[DUO]的 wfuzz 中文教程：https://www.freebuf.com/column/163553.html
HackBar 他也开始对我下手了:https://mp.weixin.qq.com/s/xWF4rAJ5xMcZmkYldBVWbg
CVE-2019-0841：Windows DACL 权限覆写权限提升漏洞:https://xz.aliyun.com/t/4784
Windows 提权笔记:https://xz.aliyun.com/t/2519
找到 CDN 背后的真实 IP:https://www.aqniu.com/threat-alert/24251.html
如何防恶意解析，禁止用 IP 访问网站的 Apache 设置？：
http://os.51cto.com/art/201307/402025.htm
Linux 如何设置只允许域名访问站点而禁止 IP 访问站点:
https://www.cnblogs.com/kimshen/p/6029778.html

工具下载网站：

知道创宇：https://github.com/knownsec
Dm2333 大佬：https://github.com/Dm2333
EventCleaner：https://github.com/360-A-Team/EventCleaner
中国蚂剑：https://github.com/AntSwordProject/antSword/releases
Windows-Exploit-Suggester：https://github.com/GDSSecurity/Windows-Exploit-Suggester
BurpSuite 破解版（含注册机，无后门）：https://blog.csdn.net/u014549283/article/details/81248886
构造优质上传漏洞 fuzz 字典：http://gv7.me/articles/2018/make-upload-vul-fuzz-dic/
一款识别图形验证码的 Burp Suite 插件：https://www.jianshu.com/p/a0262883b751
验证码识别库：http://www.wzdr.cn/article-534.html
中国特色弱口令生成器：https://github.com/RicterZ/genpAss
万能密码字典：https://wenku.baidu.com/view/d55f60e4c281e53a5902ff0d
MSDN 各种工具和服务器镜像：https://msdn.itellyou.cn/
PHP 在线加
解密网站：http://www.zhaoyuanma.com/
暴力破解工具 Hydra（九头蛇）：https://www.jianshu.com/p/e02ef0a00786
K8 工具合集：
https://github.com/k8gege/K8tools?files=1?sourceType=qq&from=singlemessage&wm=2468_90037&isappinstalled=0&featurecode=newtitle
SubFinder 是一个子域发现工具：https://github.com/subfinder/subfinder
x-pack-core-6.4.2 破解版 亲测可用:https://download.csdn.net/download/czs208112/10718181
WinAFL 模糊测试工具：https://github.com/ivanfratric/winafl
Xshell6.0 破解版本（绿色破解）:https://download.csdn.net/download/qq_32589267/10792860
应急响应工具大合集：
https://github.com/meirwah/awesome-incident-response/blob/master/README_ch.md#%E8%BF%9B%E7%A8%8BDump%E5%B7%A5%E5%85%B7
异步目标枚举工具：https://github.com/welchbj/bscan
开源扫描仪工具箱：https://github.com/We5ter/Scanners-Box
FCN：https://github.com/boywhp/fcn
slowloris.py - Python 中的简单 slowloris：https://github.com/gkbrk/slowloris

浏览器的 PWN：https://github.com/m1ghtym0/browser-pwn
SharpSploit 控制台：https://github.com/anthemtotheego/SharpSploitConsole
Wiki 收集 Red Team 基础架构强化资源：
https://github.com/bluscreenofjeff/Red-Team-Infrastructure-Wiki
CloudFlair 工具:https://github.com/christophetd/CloudFlair
高级 XSS 检测套件:https://github.com/s0md3v/XSStrike
Cooolis-ms:https://github.com/Rvn0xsy/Cooolis-ms
Ghidra 是一个软件逆向工程（SRE）框架：https://github.com/NationalSecurityAgency/ghidra

POC 框架：https://github.com/Fplyth0ner-Combie/Bug-Project-Framework
AWVS 12 下载与破解：https://blog.csdn.net/Fly_hps/article/details/85199370
红队基础设施自动化部署工具：https://github.com/QAX-A-Team/LuWu
Exploit 搜索工具 - Pompem：https://www.freebuf.com/sectool/51796.html
御剑算号工具：https://github.com/akkuman/yujian_keygen
Nessus 无 IP 限制版虚拟机-虚拟机直装版(插件更新至:http://ximcx.cn/m/?post=151
Fuzzapi:https://github.com/Fuzzapi/fuzzapi
[原创工具] 百度云网盘分享链接批量转存保存工具 10.7 修复版:
https://www.52pojie.cn/thread-804654-1-1.html
Web 版中国菜刀:https://blog.csdn.net/Kevinhanser/article/details/78010013
Burp suite 分块传输辅助插件:https://github.com/c0ny1/chunked-coding-converter

POC:

CVE-2019-9729:https://github.com/DoubleLabyrinth/SdoKeyCrypt-sys-local-privilege-elevation
CVE-2018-8453-exp:https://github.com/ze0r/cve-2018-8453-exp
CVE-2019-0841:https://github.com/rogue-kdc/CVE-2019-0841/
CVE-2019-0232:https://github.com/pyn3rd/CVE-2019-0232
CVE-2019-0192 ：https://github.com/mpgn/CVE-2019-0192
CVE-2019-0193:https://github.com/xConsole/CVE-2019-0193
CNVD-C-2019-48814.py:
https://github.com/SkewwG/VulScan/blob/master/weblogic/CNVD-C-2019-48814.py
FlexPaper <= 2.3.6 RCE 远程代码执行漏洞分析附 POC：
https://mp.weixin.qq.com/s/8eBwfW231Nm02Lz8La2P1w
elFinder 远程代码执行漏洞(CVE-2019-9194)分析复现 附:利用 POC:
https://mp.weixin.qq.com/s/20EaryilUD_jMLnR3T06Sw

7.5 闲趣文章：

2018 中国白帽人才调查报告：https://www.anquanke.com/post/id/170034
如何走进黑客世界：https://www.freebuf.com/articles/neopoints/190895.html
网络安全行业全景图：https://mp.weixin.qq.com/s/gksuSM7S-MLZ5LFz6-kjdw
《网络安全漏洞管理规定（征求意见稿）》来自站长的话:
https://bbs.wghostk.com/hacker-9420-1-1.html
刷 src 从放弃到入门:
https://zhuanlan.zhihu.com/p/36553844?utm_source=qq&utm_medium=social&utm_oi=1006149356256448512
今日威胁情报(2019/3/14):
https://mp.weixin.qq.com/s?__biz=MzUxMDk3ODEwOA==&mid=2247483949&idx=1&sn=0af897a448c8f705051f890da40d5915&chksm=f97bf37ece0c7a6864aadd8cd64c920a47ef38adb8cd61cea7afc255652702c76cd4624444a1&mpshare=1&scene=2&srcid=&from=timeline&ascene=2&devicetype=android-25&version=2700033b&nettype=cmnet&abtest_cookie=BAABAAoACwASABMABQAjlx4AVpkeAMWZHgDXmR4A3JkeAAAA&lang=zh_CN&pass_ticket=zkjIrBw5%2BKlzY3j3EZaP7HdBYdjs8WgNBud4MZf%2FJqFWT7tWGSx3Ev7o6ROFievt&wx_header=1

不积跬步，无以至千里；不积小流，无以成江海。——荀子

蓝色链接为新增链接