# 学习链接

By:梭哈王整理 +q:971841548 微信:ly331619

## web渗透测试

web全套安全资料(经典):

<https://www.cnblogs.com/hookjoy/p/7554502.html>

<https://github.com/Mosuan/collection-document>

业务逻辑漏洞:https://mp.weixin.qq.com/s/-r1oWQb\_oS8jEMdJs9Ct\_g

fiddler+burp:http://www.kali.org.cn/forum.php?mod=viewthread&tid=27363

反序列化:https://github.com/frohoff/ysoserial

struct/jboss：https://github.com/joaomatosf/jexboss

fuzz测试:twitter搜索即可，关键字加上#可搜索更多

安全从业人员常用工具以及学习指引: <https://github.com/she11c0der/Scanners-Box/blob/master/t00ls.md>

安全技能树（大赞）: <https://github.com/ym2011/SecurityTechnique>

### sql注入

注入bypass: https://github.com/0xInfection/Awesome-WAF

### xss

一个存储型xss的绕过:

https://medium.com/bugbountywriteup/story-of-a-stored-xss-bypass-26e6659f807b

### URL重定向

url 重定向绕过:https://medium.com/@malcolmx0x/three-cases-three-open-redirect-bypasses-887bda60b38c

(全面)<https://github.com/swisskyrepo/PayloadsAllTheThings/tree/master/Open%20redirect>

### 文件上传

### 1.5文件下载

### 1.6 命令执行

案例参考:https://medium.com/bugbountywriteup/command-injection-poc-72cc3743f10d

### 1.7 SSRF

百度ssrf到内网webshell: <https://shuimugan.com/bug/view?bug_no=99070>

### 1.8 指纹检测

Cms识别:

Waf识别:

### 1.9 子域名收集

### 1.10 目录扫描

<https://github.com/tengzhangchao/dirmap>

## 2、内网渗透

徐炎内网渗透：<https://www.bilibili.com/video/av37175514?t=49>

Micpoor内网渗透: https://github.com/Micropoor/Micro8

内网渗透思路：https://www.secpulse.com/archives/76810.html

powersploit=powershell+metasploit:https://www.freebuf.com/sectool/131275.html

从0开始内网渗透:https://xz.aliyun.com/t/301

meterpreter后渗透:https://www.freebuf.com/sectool/56432.html

红队与渗透测试tips: https://www.secpulse.com/archives/75843.html

域渗透体系:https://github.com/crazywa1ker/DarthSidious-Chinese

端口反弹:

https://evi1cg.me/archives/GetShellls.html

http://www.91ri.org/9367.html

https://www.t00ls.net/articles-26407.html

https://blog.csdn.net/Fly\_hps/article/details/80563579

bash/sh的shell命令解析:https://blog.csdn.net/deeplearnings/article/details/77367695

端口转发-内网漫游之sock5代理大结局:https://www.anquanke.com/post/id/85494

渗透体系的本质是知识点的串联:https://www.secpulse.com/archives/94028.html

域环境渗透测试(综合性链接)：

https://github.com/infosecn1nja/AD-Attack-Defense

http://www.fuzzysecurity.com/links.html

https://xz.aliyun.com/t/301

https://xz.aliyun.com/t/237

https://mp.weixin.qq.com/s?

\_\_biz=MzA3NzE2MjgwMg==&mid=2448903792&idx=1&sn=973719ccb5783f5af5e5f91117795f16&chksm=8b55de2d

https://mp.weixin.qq.com/s?

\_\_biz=MzA3NzE2MjgwMg==&mid=2448903792&idx=1&sn=973719ccb5783f5af5e5f91117795f16&chksm=8b55de2d

https://xz.aliyun.com/t/301

https://adsecurity.org/

http://www.fuzzysecurity.com/links.html

https://xz.aliyun.com/t/301

https://xz.aliyun.com/t/237

https://nosec.org/home/detail/2193.html

https://github.com/LOLBAS-Project/LOLBAS/blob/master/Archive-OldVersion/OSBinaries/Forfiles.exe.md

https://github.com/Ridter/Intranet\_Penetration\_Tips

https://www.anquanke.com/post/id/170471?from=timeline

https://github.com/Ridter/Intranet\_Penetration\_Tips

http://url.cn/5KtV5tw

域环境搭建:

<http://b404.xyz/2017/12/19/build-domain/>

获取系统密码：

https://times0ng.github.io/2018/04/20/Windows%E5%AF%86%E7%A0%81%E6%8A%93%E5%8F%96%E6%80%BB%E7

http://www.ansbase5.info/?p=136

https://www.freebuf.com/vuls/107340.html

https://cloud.tencent.com/developer/news/64358

openssl反弹shell: <https://medium.com/@int0x33/day-43-reverse-shell-with-openssl-1ee2574aa998>

各类杀软对应的进程名: https://www.cnblogs.com/hookjoy/p/10899119.html

### 2.1信息收集

CVE漏洞收集网站:

<http://cve.mitre.org/>

<https://www.seebug.org>

https://www.exploit-db.com/

### 2.2 漏洞利用

### 2.3 权限提升

Bypassuac: https://raw.githubusercontent.com/samratashok/nishang/master/Escalation/Invoke-PsUACme.ps1

### 2.4 横向移动

Wmic跨平台横向移动的impacket模块: https://github.com/SecureAuthCorp/impacket

### 2.5 持久控制

NET后渗透下的权限维持，附下载DLL

https://github.com/Ivan1ee/NetDLLSpy

### 2.6 痕迹清理

### 2.7 数据获取

内网密码收集脚本:

无文件免杀抓取当前机器的本地用户明文密码：

<https://raw.githubusercontent.com/EmpireProject/Empire/master/data/module_source/credentials/Invoke-Mimikatz.ps1>

https://raw.githubusercontent.com/samratashok/nishang/master/Gather/Get-PassHashes.ps1

全自动嗅探本机的各种服务明文密码:

https://github.com/DanMcInerney/net-creds

查看rdp 连接记录：

<https://raw.githubusercontent.com/klionsec/BypassAV-AllThings/master/ListLogged-inUsers.ps1>

### 2.8 内网代理

全局代理:使用proxifier

利用socks代理到内网: https://blog.csdn.net/SouthWind0/article/details/83111044

## 3、提权

### 3.1、linux

udf:http://blog.51cto.com/watertoeast/2068563 https://www.secpulse.com/archives/94028.html

https://xz.aliyun.com/t/2167?accounttraceid=85dbd2c9-8021-4125-bf50-c7be4b510695#toc-1

linux提权案例1:https://nosec.org/home/detail/2131.html

lin提权:https://shenaniganslabs.io/2019/02/13/Dirty-Sock.html Exp:https://github.com/initstring/dirty\_sock/

linux系统提权:https://payloads.online/archivers/2018-12-19/linux-privileg

### 3.2、windows

windows系统提权:

DLL劫持：

https://payloads.online/archivers/2018-12-22/1

https://payloads.online/archivers/2018-08-15/1

https://payloads.online/archivers/2018-06-09/1

https://payloads.online/archivers/2018-10-14/1

### 3.3、IIS

全版本iis提权工具(烂土豆提权):

https://www.cnblogs.com/k8gege/p/10389522.html?from=groupmessage

## 4、脚本学习

学习写poc的一些python库: 如 urllib,requests,urlparse,re,getopt，random,hashlib，base64，socket(一天学习一个)

python官方文档中文版:https://pythoncaff.com/docs/pymotw

多看python项目:https://github.com/Hood3dRob1n/JSRat-Py/blob/master/JSRat.py

powershell学习:https://www.anquanke.com/subject/id/90541

powershell：

https://github.com/search?q=powershell+bypass

https://github.com/danielbohannon/Revoke-Obfuscation?from=groupmessage

https://github.com/danielbohannon/Invoke-Obfuscation?from=groupmessage

https://www.peerlyst.com/posts/the-powershell-wiki-chiheb-chebbi

https://github.com/search?q=powershell+bypass

https://payloads.online/archivers/2018-12-18/2

nishang：https://payloads.online/archivers/2018-12-19/1

<https://blog.netwrix.com/2018/02/21/windows-powershell-scripting-tutorial-for-beginners/>

基于powershell的sock4-5的端口转发:https://raw.githubusercontent.com/p3nt4/Invoke-SocksProxy/master/InvokeSocksProxy.psm1

### Poc编写

参考pocsuite：<https://github.com/knownsec/Pocsuite>

Vulhub: <https://github.com/vulhub/vulhub>

## 5、应急响应

黑客入侵应急响应分析:

<https://www.cnblogs.com/shellr00t/p/6943796.html?utm_source=tuicool&utm_medium=referral>

高级应急响应工具:

<https://github.com/meirwah/awesome-incident-response/blob/master/README_ch.md#%E8%BF%9B%E7%A8%8BDump%E5%B7%A5%E5%85%B7>

Linux-windows应急响应.pdf

日志提取工具(好用)：https://yunpan.360.cn/surl\_yFVVmwIBJIM （提取码：4b61） 解压密码Qk7cJCCR7h3MWoR

Linux应急响应: <https://github.com/grayddq/GScan>

企业中了勒索病毒怎么办？: https://www.freebuf.com/articles/es/206199.html

## 6、日志分析

## 7、勒索病毒和远控

优秀神器大杂烩

https://github.com/quasar/QuasarRAT  
https://github.com/TheSph1nx/RT-101  
https://github.com/BlackHacker511/BlackRAT  
https://github.com/mwsrc/njRAT  
https://github.com/Jwsoat-Media/njRAT-v0.7d  
<https://github.com/zerosum0x0/koadic>

恶作剧型

https://github.com/NYAN-x-CAT/Lime-RAT 敲诈加密软件

手机远控

<https://github.com/The404Hacking/AndroRAT>

其他远控大集合

https://github.com/NYAN-x-CAT/AsyncRAT-C-Sharp  
https://github.com/heikipikker/Ender-Rat  
https://github.com/robitec97/LightCosmosRat  
https://github.com/DannyTheSloth/VanillaRat  
https://github.com/brunull/pace  
https://github.com/mvrozanti/RAT-via-Telegram  
https://github.com/Tiked/Client  
https://github.com/werkamsus/Lilith  
https://github.com/5alt/ZeroRAT  
<https://github.com/lu4p/ToRat>

远控:<https://mp.weixin.qq.com/s/hgEzZ3HhueZxAwvT7_8kbA> Ares---实践实践

关于常见勒索病毒解密软件:

<https://github.com/websec123/Decryption-Tools>

## 8、免杀和waf绕过

绕过杀软：

http://netsecurity.51cto.com/art/201702/530929.htm

免杀过av:

shellcode执行(第三方启动)开源项目:https://github.com/clinicallyinane/shellcode\_launcher/

免杀好用:

https://github.com/Arno0x/CSharpScripts https://github.com/Arno0x/ShellcodeWrapper 编译c#文件，权限有问题

### 1、shellter过av(杀毒软件):

<https://www.hackers-arise.com/evading-av-with-shellter>

### 2、wafbypass篇之web

我的wafbypass之道(misc篇)：<https://www.cnblogs.com/hookjoy/p/6579654.html>

我的wafbypass之道(upload篇): <https://www.cnblogs.com/hookjoy/p/6579646.html>

我的wafbypass之道(注入篇): <https://www.cnblogs.com/hookjoy/p/6579630.html>

Python Waf黑名单过滤下的一些ByPass思路: <http://www.0aa.me/>

### 3、免杀参考

从后渗透分析应急响应的那些事儿（二）免杀初识篇

:https://mp.weixin.qq.com/s/BBnbrDQ2EcXbz5AZF6PY8g

## 9、代码审计

php代码审计:https://www.jianshu.com/p/3f0cf18adbe7

python代码审计: https://github.com/bit4woo/python\_sec

### bypass UAC(windows防护策略)

<https://link.medium.com/bw9nIWKKHT>

## 10、甲方安全建设

安全建设:https://github.com/AnyeDuke/Enterprise-Security-Skill

日志分析:elk:https://www.elastic.co/guide/en/kibana/current/xpack-ml.html

https://blog.csdn.net/u013066244/article/details/73927756

https://www.cnblogs.com/aresxin/p/8035137.html

人人网信息安全监控:http://www.owasp.org.cn/OWASP\_Events/download/copy2\_of\_.pdf

API管理的正确姿势: <http://p.primeton.com/articles/5b02952d4be8e62df0001824>

SDL安全建设:

1、<https://xz.aliyun.com/t/226>

2、<https://www.cnblogs.com/whoami101/p/9914862.html>

日志分析:

<https://resources.infosecinstitute.com/log-analysis-web-attacks-beginners-guide/#gref>

宜信安全应急响应中心: <https://mp.weixin.qq.com/s/3TDt4veunLZkVpzRqvnd0A>

dremio，这工具可以直接使用SQL语句操作es，可以join关联：<https://www.dremio.com/download/>

安全运营:

<https://wenku.baidu.com/view/9931d63d5bcfa1c7aa00b52acfc789eb172d9e93?pcf=2>

暗网中文监控爬虫: <https://github.com/tengzhangchao/DarkNet_ChineseTrading>

Ip监控: https://github.com/grayddq/PublicMonitors/

敏感目录监控: https://github.com/tengzhangchao/dirmap

Github监控: https://github.com/ym2011/PEST/tree/master/Github-Hunter-master

Python发送邮件:

调用shodan进行实施资产监控: <https://mp.weixin.qq.com/s/_EViw4ovD27Mzjpb4mpU4g>

基于微信模板的一对多消息推送服务: <https://pushbear.ftqq.com/admin/#/>

安全管理体系建设: <https://github.com/ym2011/SecurityManagement>

## 11、ctf

https://link.medium.com/AgFOahVKHTBounty Write-up (HTB)

giuhub搜索关键字:ctf writeup

ctf-wiki(全面):https://github.com/virink/ctf-wiki

ctf-writeup(老外medium): <https://medium.com/bugbountywriteup/tagged/ctf>

KRACK-CTF:https://medium.com/bugbountywriteup/krack-jiit-ctf-writeup-92a5c2ca90c9

Veneof：<https://drive.google.com/file/d/1bmAyBWVWaLgofceIU6NeZnf4sxosohpw/view>

## 12、博客收集

安卓逆向-尼古拉斯:https://me.csdn.net/jiangwei0910410003

chybeta(全面): <https://chybeta.github.io/>

mysql蜜罐: <https://github.com/schmalle/MysqlPot>

<https://github.com/paralax/awesome-honeypots/blob/master/README_CN.md>

klion大牛博客: <https://huntingday.github.io/>

老外好用网站; <https://medium.com/bugbountywriteup>

Packet storm：<https://packetstormsecurity.com/>

墨海星辰: https://www.mzxh.xyz

暗网监控:

https://github.com/tengzhangchao/DarkNet\_ChineseTrading

<https://t.me/fordarknetspiderbot>

好用博客: <https://github.com/bit4woo>

## 13、数据库

### 11.1、mysql

mysql数据库之报错注入语句: https://mp.weixin.qq.com/s/YUR5Fyr1CCsUNPyi9qKcwg

## 14、优质项目及工具

IP列表进行定时端口服务扫描(好用！): <https://github.com/grayddq/PublicMonitors>

Ctf-wiki(全面): <https://github.com/virink/ctf-wiki>

PayloadsAllTheThings:https://github.com/swisskyrepo/PayloadsAllTheThings

2019年github上开源安全渗透类工具集合:

<https://mp.weixin.qq.com/s?__biz=MzU5Mzc1NTAyMQ==&mid=2247484144&idx=1&sn=b7fc5028d4447dea7e3a547cebeafa10&chksm=fe0aec12c97d6504870c6fd903481acbd641cb526500d79639f51f20664590eb97a64daa2a3c&mpshare=1&scene=23&srcid=&appinstall=0#rd>

Cobalt Strike 3.13 Crack下载链接:https://pan.baidu.com/s/1fRCW8G\_njyZTNtod9QUGgQ 密码:uuxz

Cobalt Strike环境搭建: http://suo.im/54mIL9

黑客py项目:https://github.com/Adastra-thw/pyHacks/blob/master/BasicAuth.py

Wuyun漏洞知识库(需翻墙): <https://shuimugan.com/>

世界上最好的黑客文章:

<https://medium.com/bugbountywriteup/tagged/bug-bounty>

国外漏洞平台: https://www.talosintelligence.com/vulnerability\_reports#zerodays

<https://medium.com/bugbountywriteup>

NSA开源工具: <https://github.com/NationalSecurityAgency/ghidra>

反向查CVE: <https://github.com/rfunix/Pompem>

Docker一键部署漏洞环境: <https://www.freebuf.com/sectool/165062.html>

Klion部署的内网渗透环境: https://pan.baidu.com/s/11coXSih-VJWoR76WyTc\_7g 提取码：wmxc

好用的流量脚本: <https://github.com/wupco/weblogger>

CVE-2019-0708：windows 3389漏洞

<https://github.com/n1xbyte/CVE-2019-0708/blob/master/crashpoc.py>

推送消息到微信的工具: <https://pushbear.ftqq.com/admin/#/>

Hack学习工具:<https://github.com/vitalysim/Awesome-Hacking-Resources>

Windows漏洞利用检测工具(好用)：<https://github.com/bitsadmin/wesng>

好用的wireshark分析工具: <https://github.com/pentesteracademy/patoolkit>

2019年护网攻击机ip: https://shimo.im/docs/cvVvfCPz3RogVI85/read

## 15、交流群

<https://pocketcorp.slack.com/messages/DHZABPT8E/>

## 16、APT研究

APT-34:https://github.com/blackorbird

## 17、网络钓鱼

Swake伪造邮件: <https://payloads.online/archivers/2019-05-09/1>

邮箱钓鱼:

<https://mp.weixin.qq.com/s/pcx8CleBTvrZRC3ZV_qUTQ->

Microsoft宏攻击: <https://www.n0sleep.com/?p=446>

开源钓鱼工具: <https://github.com/gophish>

Snowming钓鱼: https://shimo.im/docs/qIJD0G1DHTMbt38b/read

## 18、面试

<https://github.com/tengzhangchao/Pentest_Interview>

## 19、案例

记一次渗透实战:https://xz.aliyun.com/t/5191

亮点: sqlserver使用存储过程的注入

从外网到内网的渗透姿势分享: <https://xz.aliyun.com/t/5330>