信息搜集

某同学去面试，面试官问：

1. 拿到一个网站你首先做什么？

   信息搜集

2. 信息搜集需要做些什么？

   两大方面：技术和社工层面的信息搜集。

   需要搜集目标单位的（信息）资产和社工信息

3. 如何进行信息搜集？

   参见下方信息搜集思路。

4. 如果让你尽可能快速找到一个集团下各个信息系统的漏洞，该怎么办？

5. 如果让你对某个域名或者ip进行漏洞挖掘，该怎么办？

背景知识

信息搜集意义：找到更多攻击面（可能的脆弱点）

任务类型

1. 找某个目标网站的漏洞（给ip地址或者域名，让找漏洞）
2. 找某个单位所属网站的漏洞（给单位名称，让找漏洞）

网站的攻击面

技术和管理层面

1. 技术层面：找信息系统组件的漏洞、配置不当，包括

操作系统、（网络）服务、代码层面的漏洞和配置不当

2. 管理层面：人性弱点（社工）

信息搜集的思路

思路（针对具体某个网站或IP）

1. 翻页面，找可能漏洞利用点
2. 找CMS
3. 扫敏感目录和文件
4. 扫危险请求方式
5. 找旁站（c段、子域名）
6. 找供应链
7. 扫端口
8. 社工信息搜集（名字、联系方式等）

思路（针对某个单位或集团）

1. 搜集信息资产
    1. 找子域名（包括找C段、扫描子域名等方式实现）
    2. 找真实IP（如果遇到CDN云防护）
    3. 扫端口服务
    4. 扫危险请求方式
    5. 扫敏感目录和文件
    6. 找CMS
2. 翻页面功能，尝试漏洞利用

3. 找供应链
4. 收集社工信息（whois信息、网页信息、网页源码信息）
5. 内网信息搜集（三阶段扩展）

技术信息搜集

翻看网站页面，找到潜在的漏洞利用点（OWASP Top 10）

识别指纹：找到对应CMS（如有公开），查询历史相关漏洞。

网站架构及指纹

操作系统(TTL判断，大小写判断)、中间件、动态脚本解析器、数据库管理系统、代码

网站指纹：网站架构和网站CMS（一套代码模板，网站所有者只需要往里面填写内容就可以了），如历史上的shiro❤️fastjson❤️thinkphp❤️weblogic❤️struts2❤️等框架或组件漏洞危害很大，搜集到指纹后……

RCE、文件上传漏洞、反序列化、解析漏洞、SQLi、XSS、CSRF、SSRF、XXE、逻辑漏洞（含越权）、敏感信息泄露、缺陷组件

HTTP响应头

相关工具：nmap、wappalyzer、浏览器开发者工具、网站footer

在线工具：

- 微步社区：https://x.threatbook.cn/
- 潮汐指纹：http://finger.tidesec.com/
- 云悉指纹：https://www.yunsee.cn/

CMS历史漏洞搜索

站点CMS，已知漏洞搜索

seebug.org、 exploit-db.org

子目录或敏感文件

敏感文件包含敏感信息的文件。

什么是敏感信息：敏感信息包括但不限于：口令、密钥、证书、会话标识、许可证、隐私数据、授权凭据、个人数据等、源码文件、配置文件、日志文件、备份文件等

工具扫描

御剑后台扫描工具（不仅仅扫后台，还扫敏感目录和文件）/dirbuster

> 后台
>
> robots.txt
>
> 配置文件
>
> 备份文件：www.bak等

手工确认

网站名、网站全名、.zip、.rar、tar、bak、日期等的组合

www.gxaedu.com——》www.gxaedu.com.bak, www.gxaedu.com.tar.gz, www.gxaedu.com.bak20220902

路径泄露的信息

查看前端网页源码

生成报错信息：故意填写不存在的路径或者查看首页增加不存在参数让生成错误

phpinfo

git、svn、vim临时文件泄露源码：githack、svnhack工具，

思考

1. 什么样的网站才可能和目标网站在同一台服务器上?

   建在同一台服务器上的网站叫做旁站。

   同一家单位的网站有时是建立在同一服务器上的。

   服务器托管商的一台服务器上可能有多个公司的网站。

2. 如何找到目标网站同服务器的其他网站?

   有时，在同一个主域名（二级域名）下的其他子域名网站就在同一服务器上，大型机构尤其是互联网厂商的站通常例外。

   找子域名工具：oneforall

   www.gxaedu.com.同服的旁站可能找这个样子：xxx.gxaedu.com（xxx为其他子域名）

   在线服务找旁站（站长之家https://stool.chinaz.com/same）

3. 如何找到网站的真实ip？（如果目标网站在云防（云防护的简称）CDN后方，如何找到其真实ip直接进行信息搜集和渗透？）

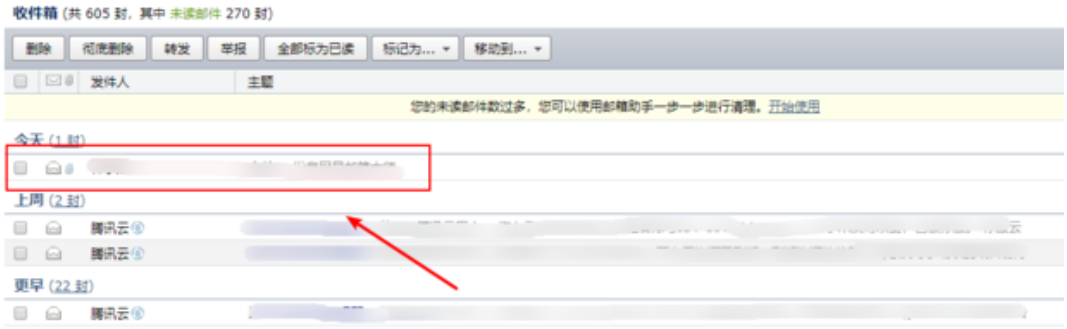
   1. 爆破不同子域名服务器的ip可能能找到；（找子域名可以通过：爬虫、资产搜索引擎、通过证书透明度计划等方式，具体参照后面找域名部分的内容）
   2. 通过邮件服务器（如果邮件服务和网站服务在同一个ip的服务器上的话）；如：mail.xxx.com和www.xxx.com在同ip服务器上，攻击者通过向某个邮箱用户（如sales@xx.com）发送邮件并且受到回复，可以通过返回的邮件信息里查看到该邮件服务器的ip，也间接查到了同服网站服务器的真实ip；

      > 步骤1

      登录QQ邮箱，点击“收件箱”

步骤2

任意选择一封朋友发来的邮件，然后点击打开



步骤3

找到右侧的三角形图标，点击打开

步骤4

点击“显示邮件原文”

> 步骤5

找到"X-Originating-IP: [... ...]"括号内的的IP就是对方发邮件时的IP地址

```
DKIM-Signature: v=1; a=rsa-sha256; c=relaxed/relaxed; d=163.com;
        s=s110527; h=Date:From:Subject:MIME-Version:Message-ID; bh=Ts6Yu
        n3UheTjGskj/D/plK1eQQ8XfVvmorp9ah6i2xc=; b=dGtXXTJGJvz7f0BKkB11j
        zUtl/O+hKEvDnfQG6r06qIaASOYj+v5B64XaUrTEFfP/bnRU+y22uIM4zTwv3M8t
        EK+YJzaeVHl3Dvk8S5MKDiE/S7EGcnejHD5SSiMy9+PEg6+ZHyIUPbZ5gbDaqhQE
        yskqkyA7cqxl7KAQUiiD34=
Received: from linzijiehandsome$163.com ( [125.65.72.77] ) by
 ajax-webmail-wmsvr59 (Coremail) ; Thu, 15 Mar 2018 21:55:10 +0800
 (GMT+08:00)
X-Originating-IP: [125.65.72.77]
Date: Thu, 15 Mar 2018 21:55:10 +0800 (GMT+08:00)
From: =?UTF-8?B?5p6X5a2Q5p2w?= <linzijiehandsome@163.com>
```

3. 通过favicon的hash值

   zoomeye.org

   fofa.info

4. 历史dns记录：https://viewdns.info/、https://x.threatbook.cn/
5. 多地进行域名解析（国外尤佳）

   多地ping：http://ping.chinaz.com/、https://ping.aizhan.com/

   www.gxaedu.com——》中国网安的WAF——》真实的服务器
6. 换协议

搜集子域名

oneforall（需要配置才能发挥全部功能哦）

御剑子域名爆破工具

subdomainbrute

以oneforall为例，使用步骤

1. 安装python脚本解析器
2. 解压缩oneforall
3. 进入oneforall目录
4. 用python执行oneforall

```
python oneforall.py --targets example.com
```

dns域传送漏洞

```
nmap --script dns-zone-transfer --script-args dns-zone-
transfer.domain=xxx.edu.cn -p 53 -Pn dns.xxx.edu.cn
```

扫端口

发现网络服务

21-23

80

3306

5432

6379

53　udp

nmap

功能：识别目标系统的操作系统、开放的端口和服务、网段中的存活主机等

-O　操作系统版本

-F 快速扫描

-A 详尽扫描

-sU UDP扫描

-Pn 无需ping通直接扫描端口

-sn　ping扫描在线情况

-iL　指定输入文件名称

-oN 指定输出文件名称

-sS 提高扫描速度

-p　指定端口（范围），默认为常见1000端口，如需扫描全端口，使用`-p 1-65535`

--min-parallelism/max-parallelism　最小最大并发数

--host-timeout 超时时长设置

-e 指定从哪个网口发包扫描

-S 指定伪造源IP

--spoof-mac　指定伪造源MAC

masscan

急速端口扫描、结果极不准确

在线服务

https://tool.chinaz.com/port/

旁站和C段

“旁站”一般指同一IP或者域名所在服务器的其他网站

在线工具

https://stool.chinaz.com/same

c段：

每个IP有ABCD四个段，举个例子，192.168.0.1，A段就是192，B段是168，C段是0，D段是1，而C段嗅探的意回思就是拿下它同一C段中的其中一台服务器答，也就是说是D段1-255中的一台服务器，然后利用工具嗅探拿下该服务。

x.x.x.x/24

ping、nslookup

whois（ip138，站长工具）

单位其他服务器

nslookup用来查询目标常见的相关记录，例如a记录、cname记录、nx记录、mx记录、ptr记录、txt/spt记录等。在最开始的被动信息搜集中，可以辅助我们搜集相关的目标记录信息。

网络空间资产搜索引擎

shadon、ZoomEye、Fofa

威胁情报

微步在线、seebug、安犬、火蚁

社工信息搜集

手工翻查页面

运维信息、联系方式等

whois：

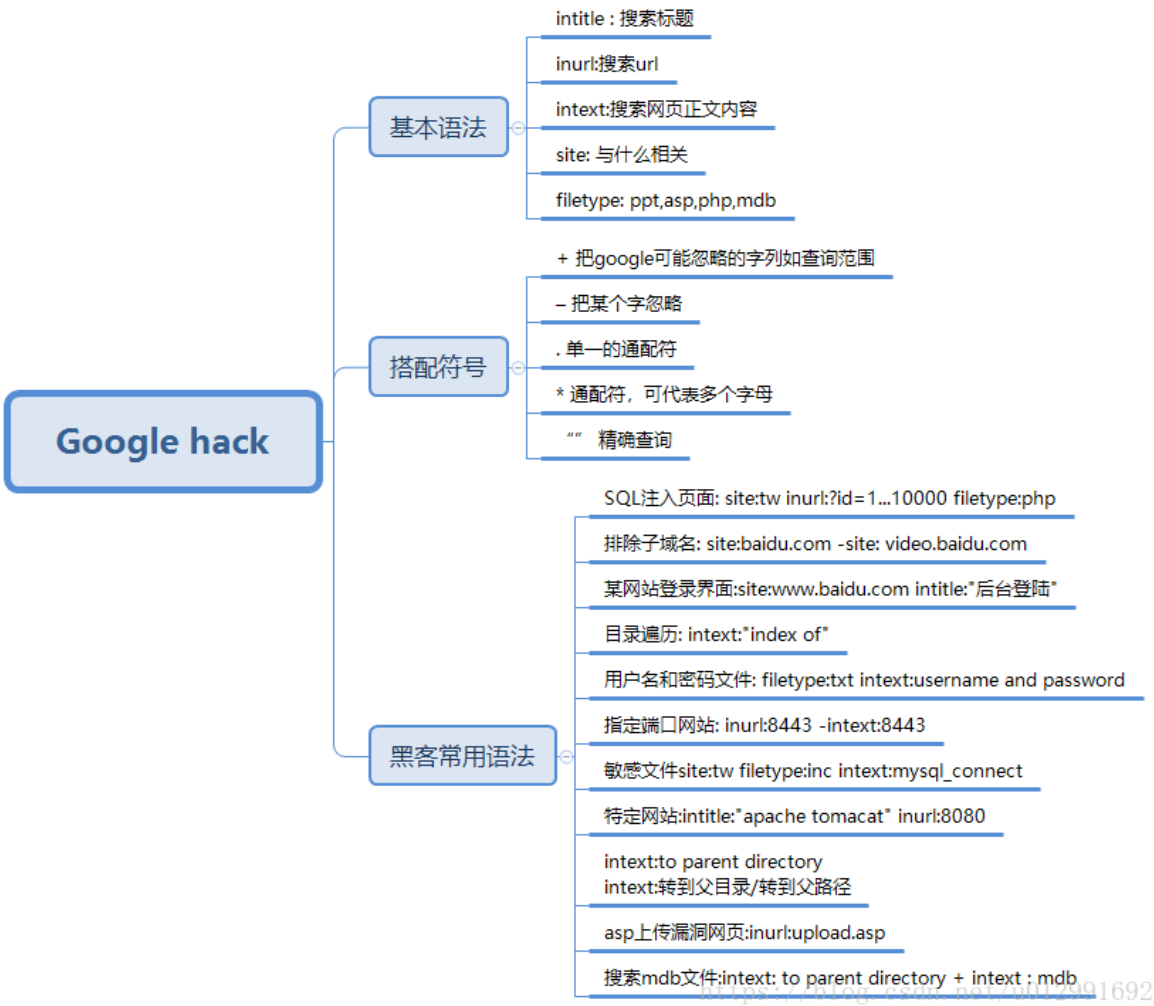
谷歌黑客google hacking

http://tools.bugscaner.com/google/

基本用法

关键字	功能
"xxx"	双引号内的内容不可拆分
site	指定域名

关键字	功能
inurl	url存在关键字的网页
intext	网页正文中的关键字
filetype	指定文件类型
intitle	网页标题中的关键字
link	link:gxaedu.com表示所有和gxaedu.com做了链接的url
info	查找指定站点的一些基本信息



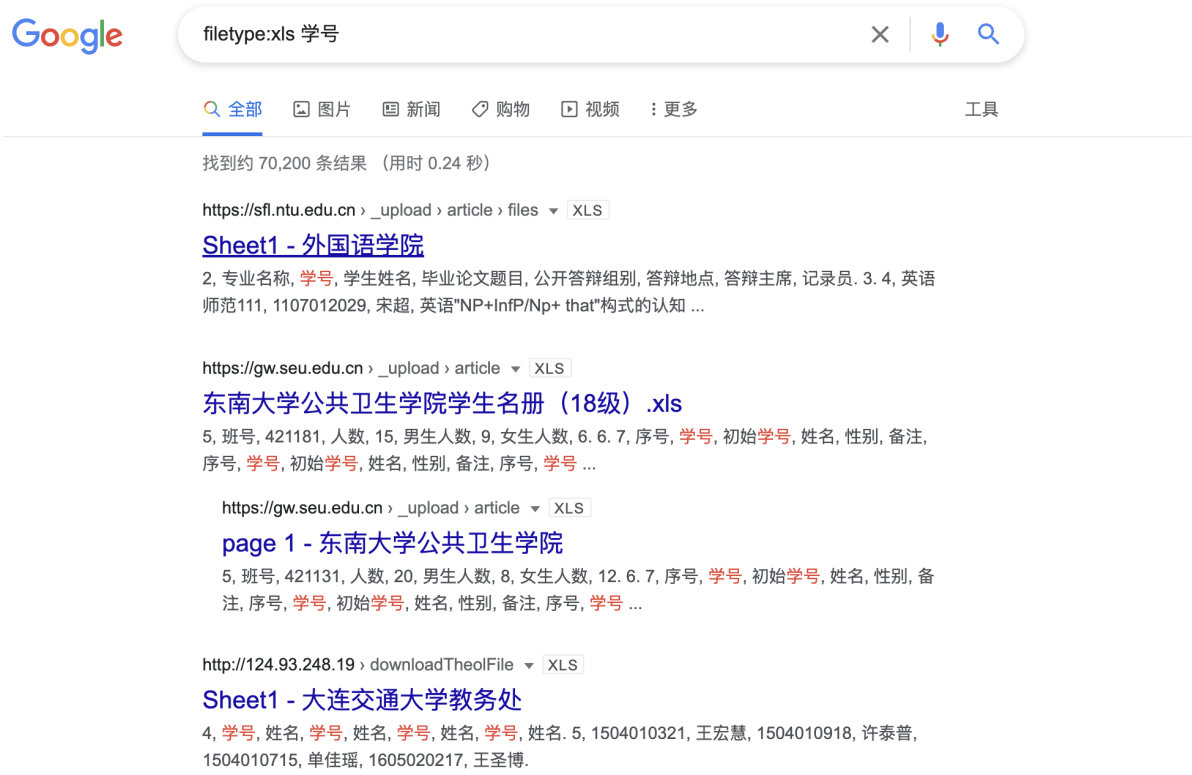
复杂用法

搜索敏感文件	搜索管理后台	搜索mail
site:xxx.com filetype:doc intext:pass	site:xxx.com 管理	site:xxx.com intext:@xxx.com
site:xxx.com filetype:xls intext:pass	site:xxx.com admin	intext:@xxx.com
site:xxx.com filetype:conf	site:xxx.com login	
site:xxx.com filetype:inc		

搜索敏感文件	搜索管理后台	搜索mail
……	……	……

搜索敏感web路径
site:xxx.com intitle:mongod inurl:28017
site:xxx.com inurl:sql.php
site:xxx.com inur:phpinfo.php
……

Google镜像站推荐：http://tools.bugscaner.com/google/



nslookup、dig

github.com

备案信息查看

https://www.beian88.com/、https://beian.miit.gov.cn/#/Integrated/index、

公司、老板信息

https://www.tianyancha.com/、https://www.17ce.com/

- 公司地址
- 公司组织架构
- 联系电话/传真号码

- 人员姓名/职务
- 公开的商业信息

源码

根据公司信息、CMS信息寻找源码

构造的社工字典（包含弱密码）

```
1
```

不同场景下的信息搜集

获取授权

打站点：

打多个站：编写脚本批量进行信息搜集

打区域：shodan、fofa、zoomeye

CTF：

AWD：先（或同时）打补丁

供应链攻击

代码审计

配置不当

多余服务

预留后门

工具

wafw00f

参考端口表

windows操作系统

服务名称	端口	服务说明	关闭方法	处置建议
系统服务部分				
echo	7/TCP	RFC862_回声协议	关闭"Simple TCP/IP Services"服务。	建议关闭
echo	7/UDP	RFC862_回声协议		
discard	9/UDP	RFC863 废除协议		
discard	9/TCP	RFC863 废除协议		
daytime	13/UDP	RFC867 白天协议		
daytime	13/TCP	RFC867 白天协议		
qotd	17/TCP	RFC865 白天协议的引用		

服务名称	端口	服务说明	关闭方法	处置建议
qotd	17/UDP	RFC865 白天协议的引用		
chargen	19/TCP	RFC864 字符产生协议		
chargen	19/UDP	RFC864 字符产生协议		
ftp	21/TCP	文件传输协议(控制)	关闭"FTP Publishing Service"服务。	根据情况选择开放
smtp	25/TCP	简单邮件发送协议	关闭"Simple Mail Transport Protocol"服务。	建议关闭
nameserver	42/TCP	WINS 主机名服务	关闭"Windows Internet Name Service"服务。	建议关闭
42/UDP				
domain	53/UDP	域名服务器	关闭"DNS Server"服务。	根据情况选择开放
53/TCP	根据情况选择开放			
dhcps	67/UDP	DHCP 服务器/Internet 连接共享	关闭"Simple TCP/IP Services"服务。	建议关闭
dhcpc	68/UDP	DHCP协议客户端	关闭"DHCP Client"服务。	建议关闭
http	80/TCP	HTTP 万维网发布服务	关闭"World Wide Web Publishing Service"服务。	根据情况选择开放
epmap	135/TCP	RPC服务	系统基本服务	无法关闭
135/UDP	无法关闭			
netbios-ns	137/UDP	NetBIOS 名称解析	在网卡的TCP/IP选项中"WINS"页勾选"禁用TCP/IP上的NETBIOS"	根据情况选择开放
netbios-dgm	138/UDP	NetBIOS 数据报服务	根据情况选择开放	
netbios-ssn	139/TCP	NetBIOS 会话服务	系统基本服务	无法关闭
snmp	161/UDP	SNMP 服务	关闭"SNMP "服务	根据情况选择开放
https	443/TCP	安全超文本传输协议	关闭"World Wide Web Publishing Service"服务	根据情况选择开放
microsoft-ds	445/UDP	SMB 服务器	运行regedit，打开HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetBT\Parameters添加名为"SMBDeviceEnabled"的子键，类型dword，值为0重新启动计算机	根据情况选择开放
445/TCP				
isakmp	500/UDP	IPSec ISAKMP 本地安全机构	关闭"IPSEC Policy Agent"服务	很少使用的服务，如不使用ipsec，建议关闭
RADIUS	1645/UDP	旧式 RADIUS Internet 身份验证服务	关闭"Remote Access Connection Manager"服务	建议关闭
RADIUS	1646/UDP	旧式 RADIUS Internet 身份验证服务	建议关闭	
radius	1812/UDP	身份验证 Internet 身份验证服务	建议关闭	
radacct	1813/UDP	计帐 Internet 身份验证服务	建议关闭	
MSMQ-RPC	2105/TCP	MSMQ-RPC 消息队列	关闭"Message Queuing"服务。	建议关闭
Termsrv	3389/TCP	终端服务	关闭"Terminal Services"服务。	根据情况选择开放
其他常用服务				
Apache	80/TCP 8000/TCP	Apache HTTP 服务器	关闭"Apache2"服务。	根据情况选择开放

服务名称	端口	服务说明	关闭方法	处置建议
ms-sql-s	1433/TCP 1434/UDP	微软公司数据库	关闭"MSSQLServer"服务。	根据情况选择开放
ORACLE	1521/TCP	甲骨文公司数据库	关闭"OracleOraHome90TNSListener"服务。	根据情况选择开放
remote administrator	4899/TCP	Famatech公司远程控制软件	关闭"Remote Administrator Service "服务。	根据情况选择开放
sybase	5000/TCP	Sybase公司数据库	关闭"Sybase SQLServer"字样开始的服务。	根据情况选择开放
pcAnywhere	5631/TCP 5632/UDP	Symantec公司远程控制软件	关闭"pcAnywhere Host Service"字样开始的服务。	根据情况选择开放

linux操作系统

服务名称	端口	应用说明	关闭方法	处置建议
daytime	13/tcp	RFC867 白天协议	chkconfig daytime off	建议关闭
13/udp	RFC867 白天协议	chkconfig daytime off		
time	37/tcp	时间协议	chkconfig time off	
37/udp	时间协议	chkconfig time-udp off		
echo	7/tcp	RFC862_回声协议	chkconfig echo off	
7/udp	RFC862_回声协议	chkconfig echo-udp off		
discard	9/tcp	RFC863 废除协议	chkconfig discard off	
9/udp	chkconfig discard-udp off			
chargen	19/tcp	RFC864 字符产生协议	chkconfig chargen off	
19/udp	chkconfig chargen-udp off			
ftp	21/tcp	文件传输协议(控制)	chkconfig gssftp off	根据情况选择开放
telnet	23/tcp	虚拟终端协议	chkconfig krb5-telnet off	根据情况选择开放

服务名称	端口	应用说明	关闭方法	处置建议
sendmail	25/tcp	简单邮件发送协议	chkconfig sendmail off	建议关闭
nameserver	53/udp	域名服务	chkconfig named off	根据情况选择开放
53/tcp	域名服务	chkconfig named off	根据情况选择开放	
apache	80/tcp	HTTP 万维网发布服务	chkconfig httpd off	根据情况选择开放
login	513/tcp	远程登录	chkconfig login off	根据情况选择开放
shell	514/tcp	远程命令, no passwd used	chkconfig shell off	根据情况选择开放
exec	512/tcp	remote execution, passwd required	chkconfig exec off	根据情况选择开放
ntalk	518/udp	new talk, conversation	chkconfig ntalk off	建议关闭
ident	113/tcp	auth	chkconfig ident off	建议关闭
printer	515/tcp	远程打印缓存	chkconfig printer off	强烈建议关闭
bootps	67/udp	引导协议服务端	chkconfig bootps off	建议关闭
68/udp	引导协议客户端	chkconfig bootps off	建议关闭	
tftp	69/udp	普通文件传输协议	chkconfig tftp off	强烈建议关闭
kshell	544/tcp	Kerberos remote shell -kfall	chkconfig kshell off	建议关闭
klogin	543/tcp	Kerberos rlogin -kfall	chkconfig klogin off	建议关闭
portmap	111/tcp	端口映射	chkconfig portmap off	根据情况选择开放
snmp	161/udp	简单网络管理协议（Agent）	chkconfig snmp off	根据情况选择开放
snmp trap	161/tcp	简单网络管理协议（Agent）	chkconfig snmp off	根据情况选择开放

服务名称	端口	应用说明	关闭方法	处置建议
snmp-trap	162/udp	简单网络管理协议（Traps）	chkconfig snmptrap off	根据情况选择开放
syslogd	514/udp	系统日志服务	chkconfig syslog off	建议保留
lpd	515/tcp	远程打印缓存	chkconfig lpd off	强烈建议关闭
nfs	2049/tcp	NFS远程文件系统	chkconfig nfs off	强烈建议关闭
2049/udp	NFS远程文件系统	chkconfig nfs off	强烈建议关闭	
nfs.lock	动态端口	rpc服务	chkconfig nfslock off	强烈建议关闭
ypbind	动态端口	rpc服务	chkconfig ypbind off	强烈建议关闭

Solaris操作系统

服务 名称	端口	服务说明	关闭方法	处置建议
echo	7/tcp	RFC862_回声协议	#echo stream tcp6 nowait root internal	建议关闭
7/udp	#echo dgram udp6 wait root internal			
discard	9/tcp	RFC863 废除协议	#discard stream tcp6 nowait root internal	
9/udp	RFC863 废除协议	#discard dgram udp6 wait root internal		
daytime	13/tcp	RFC867 白天协议	#daytime stream tcp6 nowait root internal	
13/udp	#daytime dgram udp6 wait root internal			
chargen	19/tcp	RFC864 字符产生协议	#chargen stream tcp6 nowait root internal	
19/udp	#chargen dgram udp6 wait root internal			
ftp	21/tcp	文件传输协议(控制)	#ftp stream tcp6 nowait root /usr/sbin/in.ftpd in.ftpd	根据情况选择开放

服务 名称	端口	服务说明	关闭方法	处置建议
telnet	23/tcp	虚拟终端协议	#telnet stream tcp6 nowait root /usr/sbin/in.telnetd in.telnetd	根据情况选择开放
smtp	25/tcp	简单邮件发送协议	/etc/rc.*d*/*s*_sendmail	建议关闭
time	37/tcp	时间服务	#time stream tcp6 nowait root internal	建议关闭
37/udp	#time dgram udp6 wait root internal			
name	42/udp	Host Name Server	#name dgram udp wait root /usr/sbin/in.tnamed in.tnamed	根据情况选择开放
finger	79/tcp	Finger Server	finger stream tcp6 nowait nobody /usr/sbin/in.fingerd in.fingerd	高危险服务，建议关闭
http	80/tcp	HTTP	#http stream tcp nowait nobody /opt/webserver/bin/httpd httpd	强烈建议关闭
sunrpc	111/tcp	sunrpc portmap	/etc/rc.*d*/*s*_rpc	根据情况选择开放
111/udp	/etc/rc.*d*/*s*_rpc	根据情况选择开放		
ntp	123/udp	Network Time Protocol	/etc/rc.*d*/*s*_ntpd	根据情况选择开放
snmp	161/udp	简单网络管理协议	/etc/rc.*d*/*s*_snmpdx	根据情况选择开放
dtlogin	177/udp	dtlogin	/etc/rc.*d*/*s*_dtlogin	根据情况选择开放
exec	512/tcp	Remote Process Execution	#exec stream tcp nowait root /usr/sbin/in.rexecd in.rexecd	根据情况选择开放
biff	512/udp	comsat	#comsat dgram udp wait root /usr/sbin/in.comsat in.comsat	建议关闭
login	513/tcp	Remote Login	#login stream tcp nowait root /usr/sbin/in.rlogind in.rlogind	根据情况选择开放
shell	514/tcp	shell	#shell stream tcp nowait root /usr/sbin/in.rshd in.rshd	根据情况选择开放
syslog	514/udp	syslogd	/etc/rc.*d*/*s*_syslog	建议保留
printer	515/tcp	spooler	#printer stream tcp6 nowait root /usr/lib/print/in.lpd in.lpd	强烈建议关闭
talk	517/udp	talk	#talk dgram udp wait root /usr/sbin/in.talkd in.talkd	建议关闭

服务 名称	端口	服务说明	关闭方法	处置建议
route	520/udp	routed	在该文件中的if前加注注释符	根据情况选择开放
uucp	540/tcp	uucp daemon	#uucp stream tcp nowait root /usr/sbin/in.uucpd in.uucpd	根据情况选择开放
submission	587/tcp	Mail Message Submission	/etc/rc.*d*/s_sendmail	根据情况选择开放
587/udp	Mail Message Submission	/etc/rc.*d*/s_sendmail	根据情况选择开放	
sm_config	603/tcp	SUNWsma	#sm_config stream tcp nowait root /opt/SUNWsma/bin/sma_configd sma_configd	根据情况选择开放
sun-dr	665/tcp	Remote Dynamic Reconfiguration	#sun-dr stream tcp wait root /usr/lib/dcs dcs	建议关闭
sdtperfme	834/udp	CDE protocol	/etc/rc.*d*/s_dtlogin	根据情况选择开放
WBEM	898/tcp	Sun wbem	/etc/rc.*d*/s_wbem	建议关闭
sdtperfmeter	953/udp	CDE sdtperfmeter	/etc/rc.*d*/s_dtlogin	根据情况选择开放
xaudio	1103/tcp	X Audio Server	#xaudio stream tcp wait root /usr/openwin/bin/Xaserver Xaserver -noauth -inetd	建议关闭
lockd	4045/tcp	NFS lock daemon/manager	/etc/rc.*d*/s_nfs.client	根据情况选择开放
WBEM	5987/tcp	Sun wbem	/etc/rc.*d*/s_wbem	建议关闭
X11	6000/tcp	X Window	/etc/rc.*d*/s_dtlogin	根据情况选择开放
dtspc	6112/tcp	CDE subprocess control	#dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd	强烈建议关闭
fs	7100/tcp	font-service	#fs stream tcp wait nobody /usr/openwin/lib/fs.auto fs	根据情况选择开放
dwhttpd	8888/tcp	dwhttpd	/etc/rc.*d*/s_ab2mgr	建议关闭
htt_serve	9010/tcp	htt_serve	/etc/rc.*d*/s_llim	建议关闭
lockd	4045/udp	NFS lock daemon/manager	/etc/rc.*d*/s_nfs.client	强烈建议关闭
clustmon	12000/tcp	SUNWmond	#clustmon stream tcp nowait root /usr/sbin/in.mond in.mond	根据情况选择开放

服务 名称	端口	服务说明	关闭方法	处置建议
ttsession	动态端口 >32768/tcp	ToolTalk	/etc/rc.*d*/s_dtlogin	强烈建议关闭
snmpXdmid	动态端口 >32768/tcp	SNMP to DMI mapper daemon	/etc/rc3.d/s*dmi	强烈建议关闭
sadmind	动态端口 >32768/TCP&udp	Solstice	#100232/10 tli rpc/udp wait root /usr/sbin/sadmind sadmind	强烈建议关闭
rquotad	动态端口 >32768/TCP&udp	rquotaprog quota rquota	#rquotad/1 tli rpc/datagram_v wait root /usr/lib/nfs/rquotad rquotad	强烈建议关闭
rusersd	动态端口 >32768/TCP&udp	rusers	#rusersd/2-3 tli rpc/datagram_v,circuit_v wait root /usr/lib/netsvc/rusers/rpc.rusersd rpc.rusersd	强烈建议关闭
sprayd	动态端口 >32768/TCP&udp	spray	#sprayd/1 tli rpc/datagram_v wait root /usr/lib/netsvc/spray/rpc.sprayd rpc.sprayd	强烈建议关闭
rwalld	动态端口 >32768/TCP&udp	rwall shutdown	#walld/1 tli rpc/datagram_v wait root /usr/lib/netsvc/rwall/rpc.rwalld rpc.rwalld	强烈建议关闭
rstatd	动态端口 >32768/TCP&udp	rstat rup perfmeter rstat_svc	#rstatd/2-4 tli rpc/datagram_v wait root /usr/lib/netsvc/rstat/rpc.rstatd rpc.rstatd	强烈建议关闭
ttdbserverd	动态端口 >32768/TCP&udp	ttdbserver tooltalk	#100083/1 tli rpc/tcp wait root /usr/dt/bin/rpc.ttdbserverd rpc.ttdbserverd	强烈建议关闭
kcms	动态端口 >32768/TCP&udp	SunKCMS Profile Server	#100221/1 tli rpc/tcp wait root /usr/openwin/bin/kcms_server kcms_server	强烈建议关闭
cachefsd	动态端口 >32768/TCP&udp	CacheFS Daemon	#100235/1 tli rpc/ticotsord wait root /usr/lib/fs/cachefs/cachefsd cachefsd	强烈建议关闭

Hp-ux操作系统

服务名称	端口	应用说明	关闭方法	处置建议
daytime	13/tcp	RFC867 白天协议	#daytime stream tcp nowait root internal	建议关闭
13/udp	RFC867 白天协议	#daytime dgram udp nowait root internal		
time	37/tcp	时间协议	#time stream tcp nowait root internal	
echo	7/tcp	RFC862_回声协议	#echo stream tcp nowait root internal	
7/udp	RFC862_回声协议	#echo dgram udp nowait root internal		
discard	9/tcp	RFC863 废除协议	#discard stream tcp nowait root internal	

服务名称	端口	应用说明	关闭方法	处置建议
9/udp	#discard dgram udp nowait root internal			
chargen	19/tcp	RFC864 字符产生协议	#chargen stream tcp nowait root internal	
19/udp	#chargen dgram udp nowait root internal			
ftp	21/tcp	文件传输协议(控制)	#ftp stream tcp nowait root /usr/lbin/ftpd	根据情况选择开放
telnet	23/tcp	虚拟终端协议	#telnet stream tcp nowait root /usr/lbin/telnetd telnetd	根据情况选择开放
sendmail	25/tcp	简单邮件发送协议	S540sendmail stop	建议关闭
nameserver	53/udp	域名服务	S370named stop	根据情况选择开放
53/tcp	域名服务	S370named stop	根据情况选择开放	
apache	80/tcp	HTTP 万维网发布服务	S825apache stop	根据情况选择开放
login	513/tcp	远程登录	#login stream tcp nowait root /usr/lbin/rlogind rlogind	根据情况选择开放

服务名称	端口	应用说明	关闭方法	处置建议
shell	514/tcp	远程命令, no passwd used	#shell stream tcp nowait root /usr/lbin/remshd remshd	根据情况选择开放
exec	512/tcp	remote execution, passwd required	#exec stream tcp nowait root /usr/lbin/rexecd rexecd	根据情况选择开放
ntalk	518/udp	new talk, conversation	#ntalk dgram udp wait root /usr/lbin/ntalkd ntalkd	建议关闭
ident	113/tcp	auth	#ident stream tcp wait bin /usr/lbin/identd identd	建议关闭
printer	515/tcp	远程打印缓存	#printer stream tcp nowait root /usr/sbin/rlpdaemon rlpdaemon -i	强烈建议关闭
bootps	67/udp	引导协议服务端	#bootps dstream tdp nowait root internal	建议关闭
68/udp	引导协议客户端	#bootps dgram udp nowait root internal	建议关闭	
tftp	69/udp	普通文件传输协议	#tftp dgram udp nowait root internal	强烈建议关闭
kshell	544/tcp	Kerberos remote shell -kfall	#kshell stream tcp nowait root /usr/lbin/remshd remshd -K	建议关闭
klogin	543/tcp	Kerberos rlogin -kfall	#klogin stream tcp nowait root /usr/lbin/rlogind rlogind -K	建议关闭
recserv	7815/tcp	X共享接收服务	#recserv stream tcp nowait root /usr/lbin/recserv recserv -display :0	建议关闭

服务名称	端口	应用说明	关闭方法	处置建议
dtspcd	6112/tcp	子进程控制	#dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd	强烈建议关闭
registrar	1712/tcp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据情况选择开放
1712/udp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar /etc/opt/resmon/lbin/registrar	根据情况选择开放	
动态端口	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据情况选择开放	
portmap	111/tcp	端口映射	S590Rpcd stop	根据情况选择开放
dced	135/tcp	DCE RPC daemon	S570dce stop	建议关闭
dced	135/udp	DCE RPC daemon	S570dce stop	建议关闭
snmp	161/udp	简单网络管理协议（Agent）	S560SnmpMaster stop S565OspfMib stop S565SnmpHpunix stop S565SnmpMib2 stop	根据情况选择开放
snmpd	7161/tcp	简单网络管理协议（Agent）	S560SnmpMaster stop S565OspfMib stop S565SnmpHpunix stop S565SnmpMib2 stop	根据情况选择开放
snmp-trap	162/udp	简单网络管理协议（Traps）	S565SnmpTrpDst stop	根据情况选择开放

服务名称	端口	应用说明	关闭方法	处置建议
dtlogin	177/udp	启动图形控制	S900dtlogin.rc stop	根据情况选择开放
6000/tcp	X 窗口服务	S990dtlogin.rc stop	根据情况选择开放	
动态端口	启动图形控制	S900dtlogin.rc stop	根据情况选择开放	
syslogd	514/udp	系统日志服务	S220syslogd stop	建议保留
lpd	515/tcp	远程打印缓存	S720lp stop	强烈建议关闭
router	520/udp	路由信息协议	S510gated stop	根据情况选择开放
nfs	2049/tcp	NFS远程文件系统	S100nfs.server stop	强烈建议关闭
2049/udp	NFS远程文件系统	S100nfs.server stop	强烈建议关闭	
rpc.mount	动态端口	rpc服务	S430nfs.client stop	强烈建议关闭
rpc.statd	动态端口	rpc服务	S430nfs.client stop	强烈建议关闭
rpc.lockd	动态端口	rpc服务	S430nfs.client stop	强烈建议关闭
rpc.ruserd	动态端口	rpc服务	#rpc dgram udp wait root /usr/lib/netsvc/rusers/rpc.rusersd 100002 1-2 rpc.rusersd	强烈建议关闭

服务名称	端口	应用说明	关闭方法	处置建议
rpc.yppasswd	动态端口	rpc服务	S410nis.server stop	强烈建议关闭
swagentd	2121/tcp	sw代理	S870swagentd stop	根据情况选择开放
2121/udp	sw代理	S870swagentd stop	根据情况选择开放	
rbootd	68/udp	remote boot server	START_RBOOTD 0	建议关闭
1068/udp	remote boot server	START_RBOOTD 0	建议关闭	
instl_boots	1067/udp	安装引导协议服务installation bootstrap protocol server	#instl_boots dgram udp wait root /usr/lbin/instl_bootd instl_bootd	建议关闭
1068/udp	安装引导协议服务installation bootstrap protocol client	#instl_bootc dgram udp wait root /usr/lbin/instl_bootc instl_bootc	建议关闭	
samd	3275/tcp	system mgmt daemon	samd:23456:respawn:/usr/sam/lbin/samd # system mgmt daemon	建议关闭
swat	901/tcp	SAMBA Web-based Admin Tool	swat stream tcp nowait.400 root /opt/samba/bin/swat swat	强烈建议关闭
xntpd	123/udp	时间同步服务	/sbin/rc3.d/S660xntpd stop	根据情况选择开放
rpc.ttdbserver	动态端口	HP-UX ToolTalk database server	#rpc xti tcp swait root /usr/dt/bin/rpc.ttdbserver 100083 1 /usr/dt/bin/rpc.ttdbserver	强烈建议关闭
rpc.cmsd	动态端口	后台进程管理服务	#rpc dgram udp wait root /usr/dt/bin/rpc.cmsd 100068 2-5 rpc.cmsd	强烈建议关闭

服务名称	端口	应用说明	关闭方法	处置建议
dmisp	动态端口		/sbin/rc2.d/S605Dmisp stop	强烈建议关闭
diagmond	1508/tcp	硬件诊断监控程序	S742diagnostic stop	根据情况选择开放
diaglogd	动态端口	硬件诊断程序	S742diagnostic stop	根据情况选择开放
memlogd	动态端口	内存记录服务	S742diagnostic stop	根据情况选择开放
cclogd	动态端口	chassis code logging daemon	S742diagnostic stop	根据情况选择开放
dm_memory	动态端口	Memory Monitor	S742diagnostic stop	根据情况选择开放
RemoteMonitor	2818/tcp		S742diagnostic stop	根据情况选择开放

服务名称	端口	应用说明	关闭方法	处置建议
psmctd	动态端口	Peripheral Status Monitor client/target	S742diagnostic stop	根据情况选择开放
psmond	1788/tcp	Predictive Monitor	S742diagnostic stop	根据情况选择开放
1788/udp	Hardware Predictive Monitor	S742diagnostic stop	根据情况选择开放	
hacl-hb	5300/tcp	High Availability (HA) Cluster heartbeat	S800cmcluster stop	根据情况选择开放
hacl-gs	5301/tcp	HA Cluster General Services	S800cmcluster stop	根据情况选择开放
hacl-cfg	5302/tcp	HA Cluster TCP configuration	S800cmcluster stop	根据情况选择开放
5302/udp	HA Cluster UDP configuration	S800cmcluster stop	根据情况选择开放	
hacl-local	5304/tcp	HA Cluster Commands	S800cmcluster stop	根据情况选择开放
clvm-cfg	1476/tcp	HA LVM configuration	S800cmcluster stop	根据情况选择开放

附表5：端口及服务(AIX操作系统)

服务名称	端口	应用说明	关闭方法	处置建议
daytime	13/tcp	RFC867 白天协议	#daytime stream tcp nowait root internal	建议关闭
13/udp	RFC867 白天协议	#daytime dgram udp nowait root internal		
time	37/tcp	时间协议	#time stream tcp nowait root internal	
echo	7/tcp	RFC862_回声协议	#echo stream tcp nowait root internal	
7/udp	RFC862_回声协议	#echo dgram udp nowait root internal		
discard	9/tcp	RFC863 废除协议	#discard stream tcp nowait root internal	
9/udp	#discard dgram udp nowait root internal			
chargen	19/tcp	RFC864 字符产生协议	#chargen stream tcp nowait root internal	
19/udp	#chargen dgram udp nowait root internal			
ftp	21/tcp	文件传输协议(控制)	#ftp stream tcp nowait root /usr/lbin/ftpd	根据情况选择开放
telnet	23/tcp	虚拟终端协议	#telnet stream tcp nowait root /usr/lbin/telnetd telnetd	根据情况选择开放
sendmail	25/tcp	简单邮件发送协议	rc.tcpip/sendmail	建议关闭

服务名称	端口	应用说明	关闭方法	处置建议
names	53/udp	域名服务	/etc/rc.tcpip	根据情况选择开放
53/tcp	域名服务	/etc/rc.tcpip	根据情况选择开放	
login	513/tcp	远程登录	#login stream tcp nowait root /usr/lbin/rlogind rlogind	根据情况选择开放
shell	514/tcp	远程命令, no passwd used	#shell stream tcp nowait root /usr/lbin/remshd remshd	根据情况选择开放
exec	512/tcp	remote execution, passwd required	#exec stream tcp nowait root /usr/lbin/rexecd rexecd	根据情况选择开放
ntalk	518/udp	new talk, conversation	#ntalk dgram udp wait root /usr/lbin/ntalkd ntalkd	建议关闭
ident	113/tcp	auth	#ident stream tcp wait bin /usr/lbin/identd identd	建议关闭
lpd	515/tcp	远程打印缓存	#printer stream tcp nowait root /usr/sbin/rlpdaemon rlpdaemon -i	强烈建议关闭

服务名称	端口	应用说明	关闭方法	处置建议
tftp	69/udp	普通文件传输协议	#tftp dgram udp nowait root internal	强烈建议关闭
kshell	544/tcp	Kerberos remote shell -kfall	#kshell stream tcp nowait root /usr/lbin/remshd remshd -K	建议关闭
klogin	543/tcp	Kerberos rlogin -kfall	#klogin stream tcp nowait root /usr/lbin/rlogind rlogind -K	建议关闭
recserv	7815/tcp	X共享接收服务	#recserv stream tcp nowait root /usr/lbin/recserv recserv -display :0	建议关闭
dtspcd	6112/tcp	子进程控制	#dtspc stream tcp nowait root /usr/dt/bin/dtspcd /usr/dt/bin/dtspcd	强烈建议关闭
registrar	1712/tcp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据情况选择开放
1712/udp	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar /etc/opt/resmon/lbin/registrar	根据情况选择开放	
动态端口	资源监控服务	#registrar stream tcp nowait root /etc/opt/resmon/lbin/registrar #/etc/opt/resmon/lbin/registrar	根据情况选择开放	
portmap	111/tcp	端口映射	/etc/rc.tcpip	根据情况选择开放

服务名称	端口	应用说明	关闭方法	处置建议
snmp	161/udp	简单网络管理协议（Agent）	rc.tcpip/snmpd	根据情况选择开放
snmp	7161/tcp	简单网络管理协议（Agent）	rc.tcpip/snmpd	根据情况选择开放
snmp-trap	162/udp	简单网络管理协议（Traps）	rc.tcpip/snmpd	根据情况选择开放
dtlogin	177/udp	启动图形控制	usr/dt/config/Xaccess	根据情况选择开放
6000/tcp	X 窗口服务	usr/dt/config/Xaccess	根据情况选择开放	
动态端口	启动图形控制	usr/dt/config/Xaccess	根据情况选择开放	
syslogd	514/udp	系统日志服务	/etc/rc.tcpip	建议保留
nfs	2049/tcp	NFS远程文件系统	/etc/rc.nfs	强烈建议关闭
2049/udp	NFS远程文件系统	/etc/rc.nfs	强烈建议关闭	

服务名称	端口	应用说明	关闭方法	处置建议
rpc.ttdbserver	动态端口	HP-UX ToolTalk database server	#rpc xti tcp swait root /usr/dt/bin/rpc.ttdbserver 100083 1 /usr/dt/bin/rpc.ttdbserver	强烈建议关闭
rpc.cmsd	动态端口	后台进程管理服务	#rpc dgram udp wait root /usr/dt/bin/rpc.cmsd 100068 2-5 rpc.cmsd	强烈建议关闭

参考连接：https://zhuanlan.zhihu.com/p/147374260