总结一下常见的TCP端口以及这些端口可以利用的点。

一、端口利用

端口	服务	入侵方式
21	ftp/tftp/vsftpd文件传输协议	爆破/嗅探/溢出/后门
22	ssh远程连接	爆破/openssh漏洞
23	Telnet远程连接	爆破/嗅探/弱口令
25	SMTP邮件服务	邮件伪造
53	DNS域名解析系统	域传送/劫持/缓存投毒/欺骗
67/68	dhcp服务	劫持/欺骗
110	pop3	爆破/嗅探
139	Samba服务	爆破/未授权访问/远程命令执行
143	Imap协议	爆破
161	SNMP协议	爆破/搜集目标内网信息
389	Ldap目录访问协议	注入/未授权访问/弱口令
445	smb	ms17-010/端口溢出
512/513/514	Linux Rexec服务	爆破/Rlogin登陆
873	Rsync服务	文件上传/未授权访问
1080	socket	爆破
1352	Lotus domino邮件服务	爆破/信息泄漏
1433	mssql	爆破/注入/SA弱口令
1521	oracle	爆破/注入/TNS爆破/反弹shell
2049	Nfs服务	配置不当
2181	zookeeper服务	未授权访问
2375	docker remote api	未授权访问
3306	mysql	爆破/注入
3389	Rdp远程桌面链接	爆破/shift后门
4848	GlassFish控制台	爆破/认证绕过
5000	sybase/DB2数据库	爆破/注入/提权
5432	postgresql	爆破/注入/缓冲区溢出

端口	服务	入侵方式
5632	pcanywhere服务	抓密码/代码执行
5900	vnc	爆破/认证绕过
6379	Redis数据库	未授权访问/爆破
7001/7002	weblogic	java反序列化/控制台弱口令
80/443	http/https	web应用漏洞/心脏滴血
8069	zabbix服务	远程命令执行/注入
8161	activemq	弱口令/写文件
8080/8089	Jboss/Tomcat/Resin	爆破/PUT文件上传/反序列化
8083/8086	influxDB	未授权访问
9000	fastcgi	远程命令执行
9090	Websphere控制台	爆破/java反序列化/弱口令
9200/9300	elasticsearch	远程代码执行
11211	memcached	未授权访问
27017/27018	mongodb	未授权访问/爆破

二、常见端口

端口号码 / 层	名称	备注
1	tcpmux	TCP 端口服务多路复用
5	rje	远程作业入口
7	echo	Echo 服务
9	discard	用于连接测试的空服务
11	systat	用于列举连接了的端口的系统状态
13	daytime	给请求主机发送日期和时间
17	qotd	给连接了的主机发送每日格言
18	msp	消息发送协议
19	chargen	字符生成服务；发送无止境的字符流
20	ftp-data	FTP 数据端口
21	ftp	文件传输协议（FTP）端口；有时被文件服务协议（FSP）使用
22	ssh	安全 Shell（SSH）服务
23	telnet	Telnet 服务
25	smtp	简单邮件传输协议（SMTP）
37	time	时间协议
39	rlp	资源定位协议
42	nameserver	互联网名称服务
43	nicname	WHOIS 目录服务
49	tacacs	用于基于 TCP/IP 验证和访问的终端访问控制器访问控制系统
50	re-mail-ck	远程邮件检查协议
53	domain	域名服务（如 BIND）
63	whois++	WHOIS++，被扩展了的 WHOIS 服务
67	bootps	引导协议（BOOTP）服务；还被动态主机配置协议（DHCP）服务使用
68	bootpc	Bootstrap（BOOTP）客户；还被动态主机配置协议（DHCP）客户使用

端口号码 / 层	名称	备注
69	tftp	小文件传输协议（TFTP）
70	gopher	Gopher 互联网文档搜寻和检索
71	netrjs-1	远程作业服务
72	netrjs-2	远程作业服务
73	netrjs-3	远程作业服务
73	netrjs-4	远程作业服务
79	finger	用于用户联系信息的 Finger 服务
80	http	用于万维网（WWW）服务的超文本传输协议（HTTP）
88	kerberos	Kerberos 网络验证系统
95	supdup	Telnet 协议扩展
101	hostname	SRI-NIC 机器上的主机名服务
102	iso-tsap	ISO 开发环境（ISODE）网络应用
105	csnet-ns	邮箱名称服务器；也被 CSO 名称服务器使用
107	rtelnet	远程 Telnet
109	pop2	邮局协议版本2
110	pop3	邮局协议版本3
111	sunrpc	用于远程命令执行的远程过程调用（RPC）协议，被网络文件系统（NFS）使用
113	auth	验证和身份识别协议
115	sftp	安全文件传输协议（SFTP）服务
117	uucp-path	Unix 到 Unix 复制协议（UUCP）路径服务
119	nntp	用于 USENET 讨论系统的网络新闻传输协议（NNTP）
123	ntp	网络时间协议（NTP）
137	netbios-ns	在红帽企业 Linux 中被 Samba 使用的 NETBIOS 名称服务
138	netbios-dgm	在红帽企业 Linux 中被 Samba 使用的 NETBIOS 数据报服务
139	netbios-ssn	在红帽企业 Linux 中被 Samba 使用的NET BIOS 会话服务
143	imap	互联网消息存取协议（IMAP）

端口号码 / 层	名称	备注
161	snmp	简单网络管理协议（SNMP）
162	snmptrap	SNMP 的陷阱
163	cmip-man	通用管理信息协议（CMIP）
164	cmip-agent	通用管理信息协议（CMIP）
174	mailq	MAILQ
177	xdmcp	X 显示管理器控制协议
178	nextstep	NeXTStep 窗口服务器
179	bgp	边界网络协议
191	prospero	Cliffod Neuman 的 Prospero 服务
194	irc	互联网中继聊天（IRC）
199	smux	SNMP UNIX 多路复用
201	at-rtmp	AppleTalk 选路
202	at-nbp	AppleTalk 名称绑定
204	at-echo	AppleTalk echo 服务
206	at-zis	AppleTalk 区块信息
209	qmtp	快速邮件传输协议（QMTP）
210	z39.50	NISO Z39.50 数据库
213	ipx	互联网络分组交换协议（IPX），被 Novell Netware 环境常用的数据报协议
220	imap3	互联网消息存取协议版本3
245	link	LINK
347	fatserv	Fatmen 服务器
363	rsvp_tunnel	RSVP 隧道
369	rpc2portmap	Coda 文件系统端口映射器
370	codaauth2	Coda 文件系统验证服务
372	ulistproc	UNIX Listserv
389	ldap	轻型目录存取协议（LDAP）

端口号码 / 层	名称	备注
427	svrloc	服务位置协议（SLP）
434	mobileip-agent	可移互联网协议（IP）代理
435	mobilip-mn	可移互联网协议（IP）管理器
443	https	安全超文本传输协议（HTTP）
444	snpp	小型网络分页协议
445	microsoft-ds	通过 TCP/IP 的服务器消息块（SMB）
464	kpasswd	Kerberos 口令和钥匙改换服务
468	photuris	Photuris 会话钥匙管理协议
487	saft	简单不对称文件传输（SAFT）协议
488	gss-http	用于 HTTP 的通用安全服务（GSS）
496	pim-rp-disc	用于协议独立的多址传播（PIM）服务的会合点发现（RP-DISC）
500	isakmp	互联网安全关联和钥匙管理协议（ISAKMP）
535	iiop	互联网内部对象请求代理协议（IIOP）
538	gdomap	GNUstep 分布式对象映射器（GDOMAP）
546	dhcpv6-client	动态主机配置协议（DHCP）版本6客户
547	dhcpv6-server	动态主机配置协议（DHCP）版本6服务
554	rtsp	实时流播协议（RTSP）
563	nntps	通过安全套接字层的网络新闻传输协议（NNTPS）
565	whoami	whoami
587	submission	邮件消息提交代理（MSA）
610	npmp-local	网络外设管理协议（NPMP）本地 / 分布式排队系统（DQS）
611	npmp-gui	网络外设管理协议（NPMP）GUI / 分布式排队系统（DQS）
612	hmmp-ind	HMMP 指示 / DQS
631	ipp	互联网打印协议（IPP）
636	ldaps	通过安全套接字层的轻型目录访问协议（LDAPS）
674	acap	应用程序配置存取协议（ACAP）

端口号码 / 层	名称	备注
694	ha-cluster	用于带有高可用性的群集的心跳服务
749	kerberos-adm	Kerberos 版本5（v5）的“kadmin”数据库管理
750	kerberos-iv	Kerberos 版本4（v4）服务
765	webster	网络词典
767	phonebook	网络电话簿
873	rsync	rsync 文件传输服务
992	telnets	通过安全套接字层的 Telnet（TelnetS）
993	imaps	通过安全套接字层的互联网消息存取协议（IMAPS）
994	ircs	通过安全套接字层的互联网中继聊天（IRCS）
995	pop3s	通过安全套接字层的邮局协议版本3（POPS3）

三、 UNIX 特有的端口

以下端口是 UNIX 特有的，涉及了从电子邮件到验证不等的服务。在方括号内的名称（如 [service]）是服务的守护进程名称或它的常用别名。

端口号码 / 层	名称	注释
512/tcp	exec	用于对远程执行的进程进行验证
512/udp	biff [comsat]	异步邮件客户（biff）和服务（comsat）
513/tcp	login	远程登录（rlogin）
513/udp	who [whod]	登录的用户列表
514/tcp	shell [cmd]	不必登录的远程 shell（rshell）和远程复制（rcp）
514/udp	syslog	UNIX 系统日志服务
515	printer [spooler]	打印机（lpr）假脱机
517/udp	talk	远程对话服务和客户
518/udp	ntalk	网络交谈（ntalk），远程对话服务和客户
519	utime [unixtime]	UNIX 时间协议（utime）
520/tcp	efs	扩展文件名服务器（EFS）
520/udp	router [route, routed]	选路信息协议（RIP）
521	ripng	用于互联网协议版本6（IPv6）的选路信息协议
525	timed [timeserver]	时间守护进程（timed）
526/tcp	tempo [newdate]	Tempo
530/tcp	courier [rpc]	Courier 远程过程调用（RPC）协议
531/tcp	conference [chat]	互联网中继聊天
532	netnews	Netnews
533/udp	netwall	用于紧急广播的 Netwall
540/tcp	uucp [uucpd]	Unix 到 Unix 复制服务
543/tcp	klogin	Kerberos 版本5（v5）远程登录
544/tcp	kshell	Kerberos 版本5（v5）远程 shell
548	afpovertcp	通过传输控制协议（TCP）的 Appletalk 文件编制协议（AFP）
556	remotefs [rfs_server, rfs]	Brunhoff 的远程文件系统（RFS）

四、注册的端口

列举了由网络和软件社区向 IANA 提交的要在端口号码列表中正式注册的端口。

端口号码 / 层	名称	注释
1080	socks	SOCKS 网络应用程序代理服务
1236	bvcontrol [rmtcfg]	Garcilis Packeten 远程配置服务器
1300	h323hostcallsc	H.323 电话会议主机电话安全
1433	ms-sql-s	Microsoft SQL 服务器
1434	ms-sql-m	Microsoft SQL 监视器
1494	ica	Citrix ICA 客户
1512	wins	Microsoft Windows 互联网名称服务器
1524	ingreslock	Ingres 数据库管理系统（DBMS）锁定服务
1525	prospero-np	无特权的 Prospero
1645	datametrics [old-radius]	Datametrics / 从前的 radius 项目
1646	sa-msg-port [oldradacct]	sa-msg-port / 从前的 radacct 项目
1649	kermit	Kermit 文件传输和管理服务
1701	l2tp [l2f]	第2层隧道服务（LT2P） / 第2层转发（L2F）
1718	h323gatedisc	H.323 电讯守门装置发现机制
1719	h323gatestat	H.323 电讯守门装置状态
1720	h323hostcall	H.323 电讯主持电话设置
1758	tftp-mcast	小文件 FTP 组播
1759	mtftp	组播小文件 FTP（MTFTP）
1789	hello	Hello 路由器通信端口
1812	radius	Radius 拨号验证和记帐服务
1813	radius-acct	Radius 记帐
1911	mtp	Starlight 网络多媒体传输协议（MTP）
1985	hsrp	Cisco 热备用路由器协议
1986	licensedaemon	Cisco 许可管理守护进程
1997	gdp-port	Cisco 网关发现协议（GDP）

端口号码 / 层	名称	注释
2049	nfs [nfsd]	网络文件系统（NFS）
2102	zephyr-srv	Zephyr 通知传输和发送服务器
2103	zephyr-clt	Zephyr serv-hm 连接
2104	zephyr-hm	Zephyr 主机管理器
2401	cvspserver	并行版本系统（CVS）客户 / 服务器操作
2430/tcp	venus	用于 Coda 文件系统（codacon 端口）的 Venus 缓存管理器
2430/udp	venus	用于 Coda 文件系统（callback/wbc interface 界面）的 Venus 缓存管理器
2431/tcp	venus-se	Venus 传输控制协议（TCP）的副作用
2431/udp	venus-se	Venus 用户数据报协议（UDP）的副作用
2432/udp	codasrv	Coda 文件系统服务器端口
2433/tcp	codasrv-se	Coda 文件系统 TCP 副作用
2433/udp	codasrv-se	Coda 文件系统 UDP SFTP 副作用
2600	hpstgmgr [zebrasrv]	HPSTGMGR；Zebra 选路
2601	discp-client [zebra]	discp 客户；Zebra 集成的 shell
2602	discp-server [ripd]	discp 服务器；选路信息协议守护进程（ripd）
2603	servicemeter [ripngd]	服务计量；用于 IPv6 的 RIP 守护进程
2604	nsc-ccs [ospfd]	NSC CCS；开放式短路径优先守护进程（ospfd）
2605	nsc-posa	NSC POSA；边界网络协议守护进程（bgpd）
2606	netmon [ospf6d]	Dell Netmon；用于 IPv6 的 OSPF 守护进程（ospf6d）
2809	corbaloc	公共对象请求代理体系（CORBA）命名服务定位器
3130	icpv2	互联网缓存协议版本2（v2）；被 Squid 代理缓存服务器使用
3306	mysql	MySQL 数据库服务
3346	trnsprntproxy	Trnsprnt 代理
4011	pxe	执行前环境（PXE）服务
4321	rwhois	远程 Whois（rwhois）服务

端口号码 / 层	名称	注释
4444	krb524	Kerberos 版本5（v5）到版本4（v4）门票转换器
5002	rfe	无射频以太网（RFE）音频广播系统
5308	cfengine	配置引擎（Cfengine）
5999	cvsup [CVSup]	CVSup 文件传输和更新工具
6000	x11 [X]	X 窗口系统服务
7000	afs3-fileserver	Andrew 文件系统（AFS）文件服务器
7001	afs3-callback	用于给缓存管理器回电的 AFS 端口
7002	afs3-prserver	AFS 用户和组群数据库
7003	afs3-vlserver	AFS 文件卷位置数据库
7004	afs3-kaserver	AFS Kerberos 验证服务
7005	afs3-volser	AFS 文件卷管理服务器
7006	afs3-errors	AFS 错误解释服务
7007	afs3-bos	AFS 基本监查进程
7008	afs3-update	AFS 服务器到服务器更新器
7009	afs3-rmtsys	AFS 远程缓存管理器服务
9876	sd	会话指引器
10080	amanda	高级 Maryland 自动网络磁盘归档器（Amanda）备份服务
11371	pgpkeyserver	良好隐私（PGP） / GNU 隐私卫士（GPG）公钥服务器
11720	h323callsigalt	H.323 调用信号交替
13720	bprd	Veritas NetBackup 请求守护进程（bprd）
13721	bpdbm	Veritas NetBackup 数据库管理器（bpdbm）
13722	bpjava-msvc	Veritas NetBackup Java / Microsoft Visual C++ (MSVC) 协议
13724	vnetd	Veritas 网络工具
13782	bpcd	Vertias NetBackup
13783	vopied	Veritas VOPIED 协议
22273	wnn6 [wnn4]	假名/汉字转换系统

端口号码 / 层	名称	注释
26000	quake	Quake（以及相关的）多人游戏服务器
26208	wnn6-ds	
33434	traceroute	Traceroute 网络跟踪工具

注：/etc/services中的注释如下：端口1236被注册为“bvcontrol”，但是它也被 Gracilis Packeten 远程配置服务器使用。正式名称被列为主要名称，未注册的名称被列为别名。 在/etc/services中的注释：端口 2600 到 2606 被 zebra 软件包未经注册而使用。主要名称是被注册的名称，被 zebra 使用的未注册名称被列为别名。 /etc/services 文件中的注释：该端口被注册为 wnn6，但是还在 FreeWnn 软件包中使用了未注册的“wnn4”

五、数据报传递协议端口

显示了一个和数据报传递协议（DDP）有关的端口列表。DDP 在 AppleTalk 网络上被使用。

端口号码 / 层	名称	注释
1/ddp	rtmp	路由表管理协议
2/ddp	nbp	名称绑定协议
4/ddp	echo	AppleTalk Echo 协议
6/ddp	zip	区块信息协议

六、Kerberos（工程 Athena/MIT）端口

和 Kerberos 网络验证协议相关的端口列表。在标记的地方，v5 代表 Kerberos 版本5协议。注意，这些端口没有在 IANA 注册。

端口号码 / 层	名称	注释
751	kerberos_master	Kerberos 验证
752	passwd_server	Kerberos 口令（kpasswd）服务器
754	krb5_prop	Kerberos v5 从属传播
760	krbupdate [kreg]	Kerberos 注册
1109	kpop	Kerberos 邮局协议（KPOP）
2053	knetd	Kerberos 多路分用器
2105	eklogin	Kerberos v5 加密的远程登录（rlogin）

七、未注册的端口

一个未注册的端口列表。 Linux 系统上的服务或协议使用，运行其它操作系统的机器通信所必需的端口。

端口号码 / 层	名称	注释
15/tcp	netstat	网络状态（netstat）
98/tcp	linuxconf	Linuxconf Linux 管理工具
106	poppassd	邮局协议口令改变守护进程（POPPASSD）
465/tcp	smtps	通过安全套接字层的简单邮件传输协议（SMTPS）
616/tcp	gii	使用网关的（选路守护进程）互动界面
808	omirr [omirrd]	联机镜像（Omirr）文件镜像服务
871/tcp	supfileserv	软件升级协议（SUP）服务器
901/tcp	swat	Samba 万维网管理工具（SWAT）
953	rndc	Berkeley 互联网名称域版本9（BIND 9）远程名称守护进程配置工具
1127	sufiledbg	软件升级协议（SUP）调试
1178/tcp	skkserv	简单假名到汉字（SKK）日文输入服务器
1313/tcp	xtel	法国 Minitel 文本信息系统
1529/tcp	support [prmsd, gnatsd]	GNATS 错误跟踪系统
2003/tcp	cfinger	GNU Finger 服务
2150	ninstall	网络安装服务
2988	afbackup	afbackup 客户-服务器备份系统
3128/tcp	squid	Squid 万维网代理缓存
3455	prsvp	RSVP 端口
5432	postgres	PostgreSQL 数据库
4557/tcp	fax	FAX 传输服务（旧服务）
4559/tcp	hylafax	HylaFAX 客户-服务器协议（新服务）
5232	sgi-dgl	SGI 分布式图形库
5354	noclog	NOCOL 网络操作中心记录守护进程（noclogd）
5355	hostmon	NOCOL 网络操作中心主机监视
5680/tcp	canna	Canna 日文字符输入界面
6010/tcp	x11-ssh-offset	安全 Shell（SSH）X11 转发偏移

端口号码 / 层	名称	注释
6667	ircd	互联网中继聊天守护进程（ircd）
7100/tcp	xfs	X 字体服务器（XFS）
7666/tcp	tircproxy	Tircproxy IRC 代理服务
8008	http-alt	超文本传输协议（HTTP）的另一选择
8080	webcache	万维网（WWW）缓存服务
8081	tproxy	透明代理
9100/tcp	jetdirect [laserjet, hplj]	Hewlett-Packard (HP) JetDirect 网络打印服务
9359	mandelspawn [mandelbrot]	用于 X 窗口系统的并行 Mandelbrot 生成程序
10081	kamanda	使用 Kerberos 的 Amanda 备份服务
10082/tcp	amandaidx	Amanda 备份服务
10083/tcp	amidxtape	Amanda 备份服务
20011	isdnlog	综合业务数字网（ISDN）登录系统
20012	vboxd	ISDN 音箱守护进程（vboxd）
22305/tcp	wnn4_Kr	kWnn 韩文输入系统
22289/tcp	wnn4_Cn	cWnn 中文输入系统
22321/tcp	wnn4_Tw	tWnn 中文输入系统（台湾）
24554	binkp	Binkley TCP/IP Fidonet 邮寄程序守护进程
27374	asp	地址搜索协议
60177	tfido	Ifmail FidoNet 兼容邮寄服务
60179	fido	FidoNet 电子邮件和新闻网络

八、详细端口渗透

21端口渗透

FTP通常用作对远程服务器进行管理，典型应用就是对web系统进行管理。一旦FTP密码泄露就直接威胁web系统安全，甚至黑客通过提权可以直接控制服务器。这里剖析渗透FTP服务器的几种方法。

```
(1) 基础爆破：ftp爆破工具很多，这里我推owasp的Bruter,hydra以及msf中的ftp爆破模块。
(2) ftp匿名访问：用户名：anonymous 密码：为空或者任意邮箱
(3) 后门vsftpd ：version 2到2.3.4存在后门漏洞，攻击者可以通过该漏洞获取root权限。
(https://www.freebuf.com/column/143480.html)
(4) 嗅探：ftp使用明文传输技术（但是嗅探给予局域网并需要欺骗或监听网关），使用Cain进行渗透。
(5) ftp远程代码溢出。
(https://blog.csdn.net/weixin_42214273/article/details/82892282)

(6) ftp跳转攻击。（https://blog.csdn.net/mgxcool/article/details/48249473）
```

22端口渗透

SSH 是协议，通常使用 OpenSSH 软件实现协议应用。SSH 为 Secure Shell 的缩写，由 IETF 的网络工作小组（Network Working Group）所制定；SSH 为建立在应用层和传输层基础上的安全协议。SSH 是目前较可靠，专为远程登录会话和其它网络服务提供安全性的协议。利用 SSH 协议可以有效防止远程管理过程中的信息泄露问题。

```
(1) 弱口令，可使用工具hydra，msf中的ssh爆破模块。
(2) 防火墙SSH后门。（https://www.secpulse.com/archives/69093.html）
(3) 28退格 OpenSSL
(4) openssh 用户枚举 CVE-2018-15473。（https://www.anquanke.com/post/id/157607）
```

23端口渗透

telnet是一种旧的远程管理方式，使用telnet工具登录系统过程中，网络上传输的用户和密码都是以明文方式传送的，黑客可使用嗅探技术截获到此类密码。

```
(1) 暴力破解技术是常用的技术，使用hydra,或者msf中telnet模块对其进行破解。
(2) 在linux系统中一般采用SSH进行远程访问，传输的敏感数据都是经过加密的。而对于windows下的
telnet来说是脆弱的，因为默认没有经过任何加密就在网络中进行传输。使用cain等嗅探工具可轻松截获
远程登录密码。
```

25/465端口渗透

smtp：邮件协议，在linux中默认开启这个服务，可以向对方发送钓鱼邮件
默认端口：25（smtp）、465（smtps）

```
(1) 爆破：弱口令
(2) 未授权访问
```

53端口渗透

53端口是DNS域名服务器的通信端口，通常用于域名解析。也是网络中非常关键的服务器之一。这类服务器容易受到攻击。对于此端口的渗透，一般有三种方式。

```
1  （1）使用DNS远程溢出漏洞直接对其主机进行溢出攻击，成功后可直接获得系统权限。
   (https://www.seebug.org/vuldb/ssvid-96718)
2  （2）使用DNS欺骗攻击，可对DNS域名服务器进行欺骗，如果黑客再配合网页木马进行挂马攻击，无疑是一种杀伤力很强的攻击，黑客可不费吹灰之力就控制内网的大部分主机。这也是内网渗透惯用的技法之一。
   (https://baijiahao.baidu.com/s?id=1577362432987749706&wfr=spider&for=pc)
3  （3）拒绝服务攻击，利用拒绝服务攻击可快速的导致目标服务器运行缓慢，甚至网络瘫痪。如果使用拒绝服务攻击其DNS服务器。将导致用该服务器进行域名解析的用户无法正常上网。
   (http://www.edu.cn/xxh/fei/zxz/201503/t20150305_1235269.shtml) （4）DNS劫持。
   (https://blog.csdn.net/qq_32447301/article/details/77542474)
```

80端口渗透

80端口通常提供web服务。目前黑客对80端口的攻击典型是采用SQL注入的攻击方法，脚本渗透技术也是一项综合性极高的web渗透技术，同时脚本渗透技术对80端口也构成严重的威胁。

```
1  （1）对于windows2000的IIS5.0版本，黑客使用远程溢出直接对远程主机进行溢出攻击，成功后直接获得系统权限。
2  （2）对于windows2000中IIS5.0版本，黑客也尝试利用‘Microsoft IISCGI’文件名错误解码漏洞攻击。使用X-SCAN可直接探测到IIS漏洞。
3  （3）IIS写权限漏洞是由于IIS配置不当造成的安全问题，攻击者可向存在此类漏洞的服务器上传恶意代码，比如上传脚本木马扩大控制权限。
4  （4）普通的http封包是没有经过加密就在网络中传输的，这样就可通过嗅探类工具截取到敏感的数据。如使用Cain工具完成此类渗透。
5  （5）80端口的攻击，更多的是采用脚本渗透技术，利用web应用程序的漏洞进行渗透是目前很流行的攻击方式。
6  （6）对于渗透只开放80端口的服务器来说，难度很大。利用端口复用工具可解决此类技术难题。
7  （7）CC攻击效果不及DDOS效果明显，但是对于攻击一些小型web站点还是比较有用的。CC攻击可使目标站点运行缓慢，页面无法打开，有时还会爆出web程序的绝对路径。
```

135端口渗透

135端口主要用于使用RPC协议并提供DCOM服务，通过RPC可以保证在一台计算机上运行的程序可以顺利地执行远程计算机上的代码；使用DCOM可以通过网络直接进行通信，能够跨包括HTTP协议在内的多种网络传输。同时这个端口也爆出过不少漏洞，最严重的就是缓冲区溢出漏洞，曾经疯狂一时的‘冲击波’病毒就是利用这个漏洞进行传播的。对于135端口的渗透，黑客的渗透方法为:

```
1  （1）查找存在RPC溢出的主机，进行远程溢出攻击，直接获得系统权限。如用‘DSScan’扫描存在此漏洞的主机。对存在漏洞的主机可使用‘ms05011.exe’进行溢出，溢出成功后获得系统权限。（https://wenku.baidu.com/view/68b3340c79563c1ec5da710a.html）
2  （2）扫描存在弱口令的135主机，利用RPC远程过程调用开启telnet服务并登录telnet执行系统命令。系统弱口令的扫描一般使用hydra。对于telnet服务的开启可使用工具kali链接。（https://wenku.baidu.com/view/c8b96ae2700abb68a982fbdf.html）
```

139/445端口渗透

139端口是为‘NetBIOS SessionService’提供的，主要用于提供windows文件和打印机共享以及UNIX中的Samba服务。445端口也用于提供windows文件和打印机共享，在内网环境中使用的很广泛。这两个端口同样属于重点攻击对象，139/445端口曾出现过许多严重级别的漏洞。下面剖析渗透此类端口的基本思路。

```
1  （1）对于开放139/445端口的主机，一般尝试利用溢出漏洞对远程主机进行溢出攻击，成功后直接获得系统权限。利用msf的ms-017永恒之蓝。（https://blog.csdn.net/qq_41880069/article/details/82908131）
2  （2）对于攻击只开放445端口的主机，黑客一般使用工具‘MS06040’或‘MS08067’.可使用专用的445端口扫描器进行扫描。NS08067溢出工具对windows2003系统的溢出十分有效，工具基本使用参数在cmd下会有提示。（https://blog.csdn.net/god_7z1/article/details/6773652）
3  （3）对于开放139/445端口的主机，黑客一般使用IPC$进行渗透。在没有使用特点的账户和密码进行空连接时，权限是最小的。获得系统特定账户和密码成为提升权限的关键了，比如获得administrator账户的口令。（https://blog.warhut.cn/dmbj/145.html）
4  （4）对于开放139/445端口的主机，可利用共享获取敏感信息，这也是内网渗透中收集信息的基本途径。
```

1433端口渗透

1433是SQLServer默认的端口，SQL Server服务使用两个端口：tcp-1433、UDP-1434.其中1433用于供SQLServer对外提供服务，1434用于向请求者返回SQLServer使用了哪些TCP/IP端口。1433端口通常遭到黑客的攻击，而且攻击的方式层出不穷。最严重的莫过于远程溢出漏洞了，如由于SQL注射攻击的兴起，各类数据库时刻面临着安全威胁。利用SQL注射技术对数据库进行渗透是目前比较流行的攻击方式，此类技术属于脚本渗透技术。

```
1  （1）对于开放1433端口的SQL Server2000的数据库服务器，黑客尝试使用远程溢出漏洞对主机进行溢出测试，成功后直接获得系统权限。（https://blog.csdn.net/gxj022/article/details/4593015）
2  （2）暴力破解技术是一项经典的技术。一般破解的对象都是SA用户。通过字典破解的方式很快破解出SA的密码。（https://blog.csdn.net/kali_linux/article/details/50499576）
3  （3）嗅探技术同样能嗅探到SQL Server的登录密码。
4  （4）由于脚本程序编写的不严密，例如，程序员对参数过滤不严等，这都会造成严重的注射漏洞。通过SQL注射可间接性的对数据库服务器进行渗透，通过调用一些存储过程执行系统命令。可以使用SQL综合利用工具完成。
```

1521端口渗透

1521是大型数据库Oracle的默认监听端口，估计新手还对此端口比较陌生，平时大家接触的比较多的是Access，MSSQL以及MYSQL这三种数据库。一般大型站点才会部署这种比较昂贵的数据库系统。对于渗透这种比较复杂的数据库系统，黑客的思路如下：

```
1  （1）Oracle拥有非常多的默认用户名和密码，为了获得数据库系统的访问权限，破解数据库系统用户以及密码是黑客必须攻破的一道安全防线。
2  （2）SQL注射同样对Oracle十分有效，通过注射可获得数据库的敏感信息，包括管理员密码等。
3  （3）在注入点直接创建java，执行系统命令。（4）https://www.leiphone.com/news/201711/JjzXFp46zEPMvJod.html
4  以上的端口渗透原理只是用作分析，现在网上有很多自动的端口入侵工具，比如445批量抓鸡器或者1433批量抓鸡器。大家有兴趣的可以去网上下载试用。
```

2049端口渗透

NFS（Network File System）即网络文件系统，是FreeBSD支持的文件系统中的一种，它允许网络中的计算机之间通过TCP/IP网络共享资源。在NFS的应用中，本地NFS的客户端应用可以透明地读写位于远端NFS服务器上的文件，就像访问本地文件一样。如今NFS具备了防止被利用导出文件夹的功能，但遗留系统中的NFS服务配置不当，则仍可能遭到恶意攻击者的利用。

3306端口渗透

3306是MYSQL数据库默认的监听端口，通常部署在中型web系统中。在国内LAMP的配置是非常流行的，对于php+mysql构架的攻击也是属于比较热门的话题。对于3306端口的渗透，黑客的方法如下:

```
1  （1）由于管理者安全意识淡薄，通常管理密码设置过于简单，甚至为空口令。使用破解软件很容易破解此类密码，利用破解的密码登录远程mysql数据库，上传构造的恶意UDF自定义函数代码进行注册，通过调用注册的恶意函数执行系统命令。或者向web目录导出恶意的脚本程序，以控制整个web系统。
2  （2）功能强大的‘cain’同样支持对3306端口的嗅探，同时嗅探也是渗透思路的一种。
3  （3）SQL注入同样对mysql数据库威胁巨大，不仅可以获取数据库的敏感信息，还可使用load_file()函数读取系统的敏感配置文件或者从web数据库链接文件中获得root口令等，导出恶意代码到指定路径等。
```

3389端口渗透

3389是windows远程桌面服务默认监听的端口，管理员通过远程桌面对服务器进行维护，这给管理工作带来的极大的方便。

```
(1) 对于windows2000的旧系统版本，使用‘输入法漏洞’进行渗透。
(2) cain是一款超级的渗透工具，同样支持对3389端口的嗅探。
(3) Shift粘滞键后门：5次shift后门
(4) 社会工程学通常是最可怕的攻击技术，如果管理者的一切习惯和规律被黑客摸透的话，那么他管理的网络系统会因为他的弱点被渗透。
(5) 爆破3389端口。这里还是推荐使用hydra爆破工具。
(6) ms12_020死亡蓝屏攻击。（https://www.cnblogs.com/R-Hacker/p/9178066.html） (7) https://www.cnblogs.com/backlion/p/9429738.html
```

4899端口渗透

4899端口是remoteadministrator远程控制软件默认监听的端口，也就是平时常说的radmini影子。radmini目前支持TCP/IP协议，应用十分广泛，在很多服务器上都会看到该款软件的影子。对于此软件的渗透，思路如下：

```
(1) radmini同样存在不少弱口令的主机，通过专用扫描器可探测到此类存在漏洞的主机。
(2) radmini远控的连接密码和端口都是写入到注册表系统中的，通过使用webshell注册表读取功能可读取radmini在注册表的各项键值内容，从而破解加密的密码散列。
```

5432端口渗透

PostgreSQL是一种特性非常齐全的自由软件的对象-关系型数据库管理系统，可以说是目前世界上最先进，功能最强大的自由数据库管理系统。

```
(1) 爆破：弱口令：postgres postgres
(2) 缓冲区溢出：CVE-2014-2669。（http://drops.xmd5.com/static/drops/tips-6449.html）
(3) 远程代码执行：CVE-2018-1058。（https://www.secpulse.com/archives/69153.html）
```

5631端口渗透

5631端口是著名远程控制软件pcanywhere的默认监听端口，同时也是世界领先的远程控制软件。利用此软件，用户可以有效管理计算机并快速解决技术支持问题。由于软件的设计缺陷，使得黑客可随意下载保存连接密码的*.cif文件，通过专用破解软件进行破解。这些操作都必须在拥有一定权限下才可完成，至少通过脚本渗透获得一个webshell。通常这些操作在黑客界被称为pcanywhere提权技术。

```
PcAnyWhere提权。（https://blog.csdn.net/Fly_hps/article/details/80377199）
```

5900端口渗透

5900端口是优秀远程控制软件VNC的默认监听端口。对于该端口的渗透，思路如下：

```
1    (1) VNC软件存在密码验证绕过漏洞，此高危漏洞可以使得恶意攻击者不需要密码就可以登录到一个远程系统。
2    (2) cain同样支持对VNC的嗅探，同时支持端口修改。
3    (3) VNC的配置信息同样被写入注册表系统中，其中包括连接的密码和端口。利用webshell的注册表读取功能进行读取加密算法，然后破解。 (4) VNC拒绝服务攻击 (CVE-2015-5239) 。 (http://blogs.360.cn/post/vnc%E6%8B%92%E7%BB%9D%E6%9C%8D%E5%8A%A1%E6%BC%8F%E6%B4%9Ecve-2015-5239%E5%88%86%E6%9E%90.html)
4    (5) VNC权限提升 (CVE-2013-6886) 。
```

6379端口渗透

Redis是一个开源的使用c语言写的，支持网络、可基于内存亦可持久化的日志型、key-value数据库。

```
1    (1) 爆破：弱口令
2    (2) 未授权访问+配合ssh key提权。 (http://www.alloyteam.com/2017/07/12910/)
```

7001/7002端口渗透

7001/7002通常是weblogic中间件端口

```
1    (1) 弱口令、爆破，弱密码一般为weblogic/Oracle@123 or weblogic
2    (2) 管理后台部署 war 后门
3    (3) SSRF
4    (4) 反序列化漏洞
5    (5) weblogic_uachttps://github.com/vulhub/vulhub/tree/master/weblogic/ssrfhttps://bbs.pediy.com/thread-224954.htmhttps://fuping.site/2017/06/05/Weblogic-Vulnerability-Verification/https://blog.gdssecurity.com/labs/2015/3/30/weblogic-ssrf-and-xss-cve-2014-4241-cve-2014-4210-cve-2014-4.html
```

8080端口渗透

8080端口通常是apache_Tomcat服务器默认监听端口，apache是世界使用排名第一的web服务器。国内很多大型系统都是使用apache服务器，对于这种大型服务器的渗透，主要有以下方法：

```
(1) Tomcat远程代码执行漏洞（https://www.freebuf.com/column/159200.html）
(2) Tomcat任意文件上传。（http://liehu.tass.com.cn/archives/836）
(3) Tomcat远程代码执行&信息泄露。（https://paper.seebug.org/399/）
(4) Jboss远程代码执行。
(http://mobile.www.cnblogs.com/Safe3/archive/2010/01/08/1642371.html)
(5) Jboss反序列化漏洞。（https://www.zybuluo.com/websec007/note/838374）
(6) Jboss漏洞利用。（https://blog.csdn.net/u011215939/article/details/79141624）
```

27017端口渗透

MongoDB，NoSQL数据；攻击方法与其他数据库类似

```
(1) 爆破：弱口令
(2) 未授权访问；（http://www.cnblogs.com/LittleHann/p/6252421.html） (3)
http://www.tiejiang.org/19157.htm
```

补充阅读

https://www.freebuf.com/articles/web/284218.html