| 端口号 | 端口说明 | 攻击技巧 |
| --- | --- | --- |
| 21/22/69 | ftp/tftp：文件传输协议 | 爆破\嗅探\溢出\后门 |
| 22 | ssh：远程连接 | 爆破OpenSSH；28个退格 |
| 23 | telnet：远程连接 | 爆破\嗅探 |
| 25 | smtp：邮件服务 | 邮件伪造 |
| 53 | DNS：域名系统 | DNS区域传输\DNS劫持\DNS缓存投毒\DNS欺骗\利用DNS隧道技术刺透防火墙 |
| 67/68 | dhcp | 劫持\欺骗 |
| 110 | pop3 | 爆破 |
| 139 | samba | 爆破\未授权访问\远程代码执行 |
| 143 | imap | 爆破 |
| 161 | snmp | 爆破 |
| 389 | ldap | 注入攻击\未授权访问 |
| 512/513/514 | linux r | 直接使用rlogin |
| 873 | rsync | 未授权访问 |
| 1080 | socket | 爆破：进行内网渗透 |
| 1352 | lotus | 爆破：弱口令\信息泄漏：源代码 |
| 1433 | mssql | 爆破：使用系统用户登录\注入攻击 |
| 1521 | oracle | 爆破：TNS\注入攻击 |
| 2049 | nfs | 配置不当 |
| 2181 | zookeeper | 未授权访问 |
| 3306 | mysql | 爆破\拒绝服务\注入 |
| 3389 | rdp | 爆破\Shift后门 |
| 4848 | glassfish | 爆破：控制台弱口令\认证绕过 |
| 5000 | sybase/DB2 | 爆破\注入 |
| 5432 | postgresql | 缓冲区溢出\注入攻击\爆破：弱口令 |
| 5632 | pcanywhere | 拒绝服务\代码执行 |
| 5900 | vnc | 爆破：弱口令\认证绕过 |
| 6379 | redis | 未授权访问\爆破：弱口令 |
| 7001 | weblogic | Java反序列化\控制台弱口令\控制台部署webshell |
| 80/443/8080 | web | 常见web攻击\控制台爆破\对应服务器版本漏洞 |
| 8069 | zabbix | 远程命令执行 |
| 9090 | websphere控制台 | 爆破：控制台弱口令\Java反序列 |
| 9200/9300 | elasticsearch | 远程代码执行 |
| 11211 | memcacache | 未授权访问 |
| 27017 | mongodb | 爆破\未授权访问 |