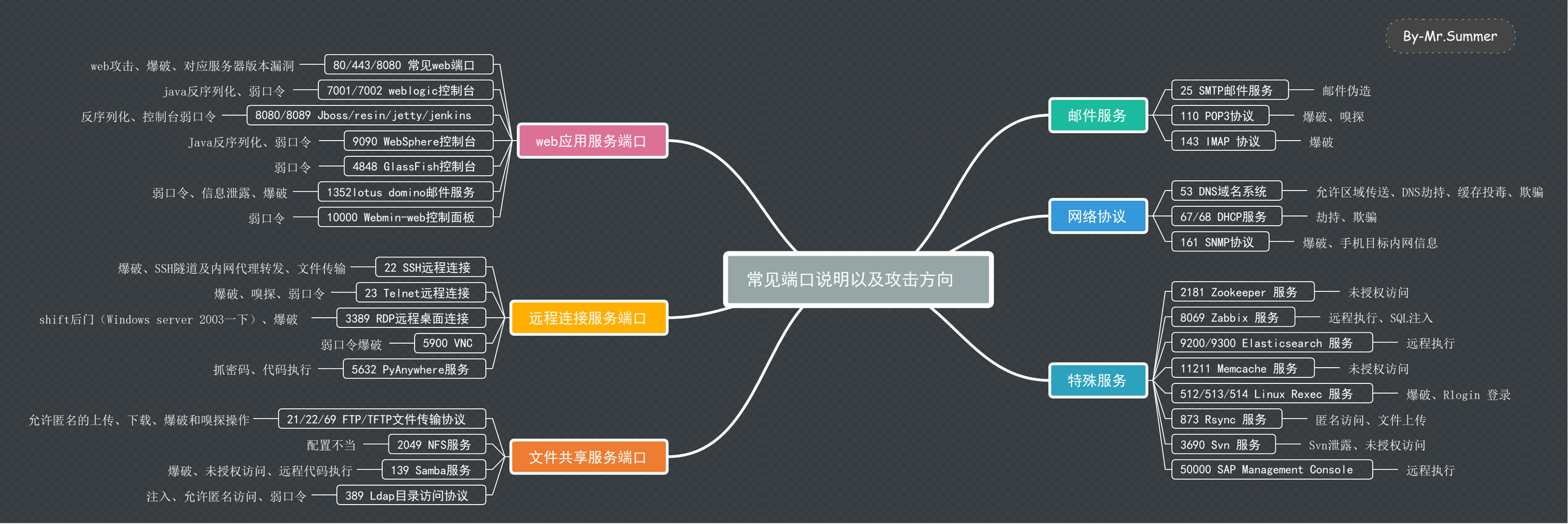
By-Mr.Summer
常见端口说明以及攻击方向
web应用服务端口
80/443/8080 常见web端口
web攻击、爆破、对应服务器版本漏洞
7001/7002 weblogic控制台
java反序列化、弱口令
8080/8089 Jboss/resin/jetty/jenkins
反序列化、控制台弱口令
9090 WebSphere控制台
Java反序列化、弱口令
4848 GlassFish控制台
弱口令
1352lotus domino邮件服务
弱口令、信息泄露、爆破
10000 Webmin-web控制面板
弱口令
远程连接服务端口
22 SSH远程连接
爆破、SSH隧道及内网代理转发、文件传输
23 Telnet远程连接
爆破、嗅探、弱口令
3389 RDP远程桌面连接
shift后门（Windows server 2003一下）、爆破
5900 VNC
弱口令爆破
5632 PyAnywhere服务
抓密码、代码执行
文件共享服务端口
21/22/69 FTP/TFTP文件传输协议
允许匿名的上传、下载、爆破和嗅探操作
2049 NFS服务
配置不当
139 Samba服务
爆破、未授权访问、远程代码执行
389 Ldap目录访问协议
注入、允许匿名访问、弱口令
邮件服务
25 SMTP邮件服务
邮件伪造
110 POP3协议
爆破、嗅探
143 IMAP 协议
爆破
网络协议
53 DNS域名系统
允许区域传送、DNS劫持、缓存投毒、欺骗
67/68 DHCP服务
劫持、欺骗
161 SNMP协议
爆破、手机目标内网信息
特殊服务
2181 Zookeeper 服务
未授权访问
8069 Zabbix 服务
远程执行、SQL注入
9200/9300 Elasticsearch 服务
远程执行
11211 Memcache 服务
未授权访问
512/513/514 Linux Rexec 服务
爆破、Rlogin 登录
873 Rsync 服务
匿名访问、文件上传
3690 Svn 服务
Svn泄露、未授权访问
50000 SAP Management Console
远程执行