nmap常用扫描命令（注意区分小写字母0和数字0，此处参数均为字母0）

-sT TCP connect()扫描，这种方式会在目标主机的日志中记录大批的链接请求以及错误信息。

-sP ping扫描，加上这个参数会使用ping扫描，只有主机存活，nmap才会继续扫描，一般最好不加，因为有的主机会禁止ping，却实际存在。

-sF -sN 秘密FIN数据包扫描，圣诞树（Xmas Tree）,空（NULL）扫描模式

-sS 半开扫描，一般不会记入日志，不过需要root权限。

-sU udp扫描，但是一般不可靠，

-sA 用来穿过防火墙的规则集，速度慢。

-sV 端口服务及版本

-A 包含了-sV，-O，全面系统检测，启动脚本检测，扫描等。

-p 指定端口，如【1-65535】，【1433，135，3389】

-P0 -Pn 扫描之前不使用ping，适用于防火墙禁止ping，比较有用。-P0和-Pn两个选项的效果是一样的，就是不进行主机发现，而直接进行更深层次的扫描，如服务版本扫描或系统类型扫描。

-v 显示扫描进程

-O 探测目标系统的漏洞，容易误报

-oN/-oX/-oG 将报告写入文件，格式分别为正常（自定义.txt）,XML,grepable.

-iL 扫描主机列表

-sC –script=default 默认的脚本扫描，主要是搜集各种应用服务的信息

-T4 禁止TCP端口禁止动态扫描延迟超时10ms，将时间设置为4，5最快

nmap扫描实例

案例一：使用nmap扫描指定IP开放端口

nmap –sS –p 1-65535 -v 192.168.0.100

使用半开扫描，指定扫描端口1到65535，-v表示显示扫描过程

案例二：扫描www.aaa.com C段存活主机

nmap –sP www.aaa.com/24 -oN nmap.txt

ping扫描该网址C段主机，并将扫描结果以TXT形式保存为桌面的nmap.txt文件

案例三：指定端口扫描

nmap –p 80，1433，3389 -v 192.168.0.100

案例四：探测主机操作系统

nmap -o www.aaa.com

案例五：全面系统探测

nmap -v -A www.aaa.com

P.S:全面系统探测，默认扫描主机的1000个高危端口，若要检测所有端口，需要加入

-p 1-65535或者-p-

案例六：穿越防火墙进行扫描

比如www.2cto.com是禁止ping的，nmap的一些常用选项无法发挥作用，可利用-Pn参数

nmap –Pn –A www.2cto.com