**一、Nmap介绍**

**Nmap英文全称是“Network Mapper”，中文为“网络映射器”。**

是一款开源代码的网络探测和安全审核的工具，它的设计目标是快速地扫描大型网络，当然用它扫描单个主机也没有问题。

诞生于1996年，著名的网络安全工具，是一个网络端口扫描以及远程操作系统、服务鉴别工具，还具备有相对完整的信息收集、数据库浸透、网络浸透测试等功能。

Nmap的“兄弟”包括NetCat（一个神奇的工具）、Nping以及Zenmap，它的“姐妹”包括Nmap.Org、SecLists.Org、SecTools.Org、Insecure.Org等著名网络安全站点。

Nmap的基本功能有3个，一是探测一组主机是否在线，其次是扫描主机端口，嗅探所提供的网络服务，还可以推断主机所用的操作系统。

Nmap输出的是扫描目标的列表，以及每个目标的补充信息，至于是哪些信息则依赖于所使用的选项。Open（开放的）意味着目标机器上的应用程序正在该端口监听连接/报文。  
Filtered（被过滤的）意味着防火墙，过滤器或者其他网络障碍阻止了该端口被访问，Namp无法得知它是OPen还是Closed。  
Closed（关闭的）端口上面没有应用程序监听，但是它们随时可能开放。  
Nmap----Script功能的使用。在Nmap的安装目录的share/nmap/scripts中。

安装Nmap：Windows、Linux/Unix、Mac OS  
注：Mac OS的安全体系默认不允许安装非安全认证的软件，这需要在系统偏好设置---安全性与隐私当中将“允许从以下位置下载的应用程序”更改为“任何来源”，即可自由安装第三方软件。  
安装地址：  
<https://nmap.org/download.html>

# 二、Nmap工作原理和语法格式

Nmap使用TCP/IP协议栈指纹准确地判断目标主机的操作系统类型，

## Nmap工作原理如下：

测试（描述）  
T1（发送TCP数据包（Flag=SYN）到开放TCP端口）  
T2（发送一个空的TCP数据包到开放的TCP端口）  
T3（发送TCP数据包（Flag=SYN，URG，PSH，FIN）到开放的TCP端口）  
T4（发送TCP数据包（Flag=ACK）到开放的TCP端口）  
T5（发送TCP数据包（Flag=SYN）到关闭的TCP端口）  
T6（发送TCP数据包（Flag=ACK）到开放的TCP端口）  
T7（发送TCP数据包（Flag=URG，PSH，FIN）到关闭的TCP端口）  
Nmap对目标主机进行一系列的测试，利用测试结果建立相应的目标主机的Nmap指纹，然后Nmap会对指纹进行匹配，最终输出相应的结果。

## Nmap固定语法格式

### Nmap【空格】【选项|多选项|协议】【空格】【目标】

其中，选项与多选项之间也是用空格进行分割的，如果某些选项需要制定某些数据，那么在这些选项与制定的数据之间也需要用空格进行分割。  
注：所有的选项与命令以及选项参数都是用空格进行分割的，有时候选项与参数直接可以不用空格分割，如-p80，-p 是选项，80 是参数。为了是Nmap语法更加严谨，建议严格按照空格进行分割。

## Nmap全面扫描的选项是-A

它可以全面扫描指定IP或域名的所有端口及其目标系统信息等，这需要花费点时间等待Nmap的扫描。  
如：nmap -A 192.168.126.116  
全面扫描又称作综合扫描，是一种完整扫描目标信息的扫描方式。

## Nmap扫描指定段

我们指定扫描一个C段，这个功能不需要其他额外的选项，只需要使用“-”进行连接。  
如：nmap 192.168.126.1-200