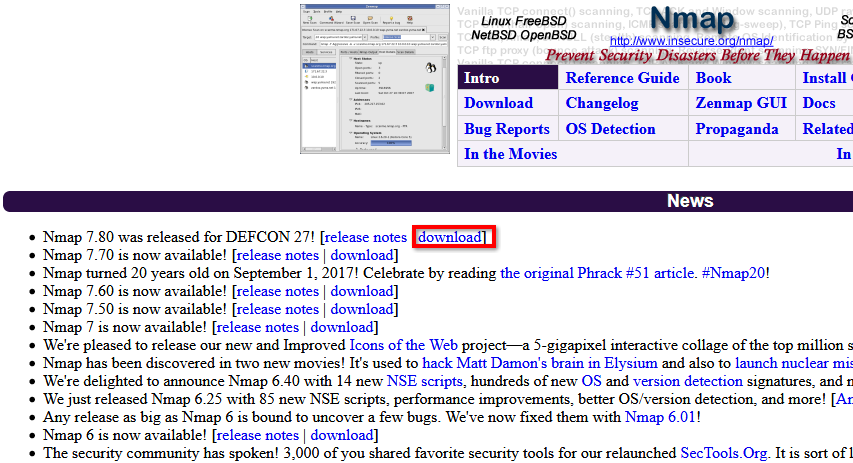
### Nmap扫描教程

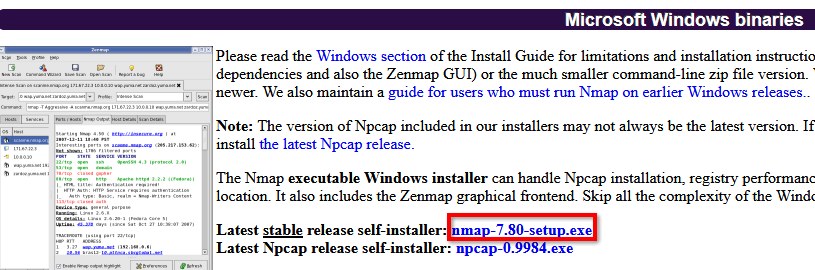
简介：nmap是一个开源的扫描工具软件，主要用来扫描目标主机或网段的主机是否在线和开放的端口以及开启的服务等信息。

**一：下载安装nmap**

Windows版本下载网址：<https://nmap.org/>



在首页里找到要使用的版本，点击download即可进行下载页，在下载页里找到windows版本的资源，点击蓝色的链接即可下载到本地。



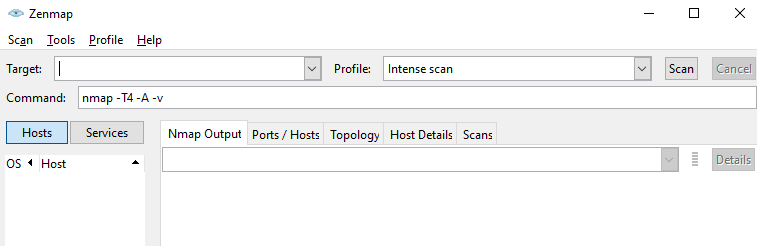
下载后，双击安装。

如果是Linux系统，直接用yum install nmap或apt-get install nmap即可。

**二：打开Nmap程序**

在桌面上找到Nmap Zenmap GUI的图标，它是nmap的可视化外壳，双击运行。





上图就是zenmap的主界面了，可以在Target：后输入目标ip或网段，在Profile：后选择扫描类型，点击Scan，就可以进行扫描。不过这个Profile扫描类型有限，也不够灵活，本教程就不教了。

本教程只教命令行的操作，操作方法是 在Command：后输入命令，按下回车即可。

如果是Linux系统，直接在console命令行里输入命令，回车即可

（有些扫描类型需要管理员权限）

**命令说明**：

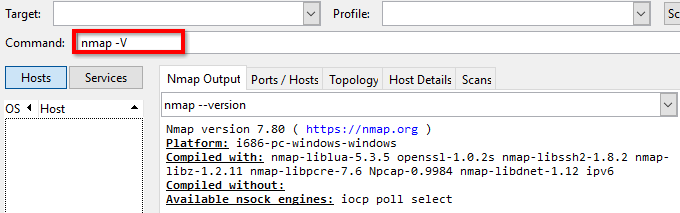
**nmap -sS等扫描参数 目标ip**

第一个单词nmap表示调用nmap这个程序，后面的参数和目标是传给这个nmap程序的，回车后执行命令。

参数可带多个，自由组合，不过有的命令不能同时使用。

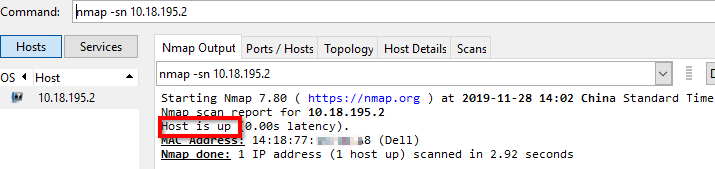
**三：Nmap扫描参数**

**nmap -V** //查看nmap版本（大写的V）,也可用 --version

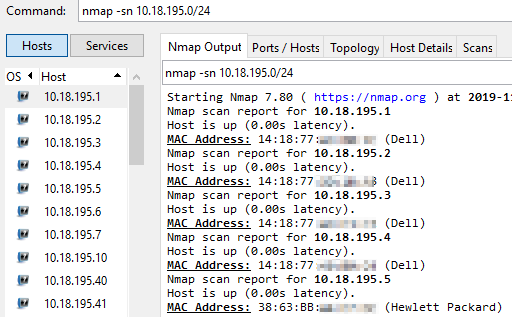


**nmap -sP 目标ip** //Ping扫描，发送icmp echo request 确认主机是否开机

//也可用 -sn 表示仅ping扫描，不扫描端口



**nmap -sn 目标网段/子网掩码位数** //扫描整个网段开机的主机

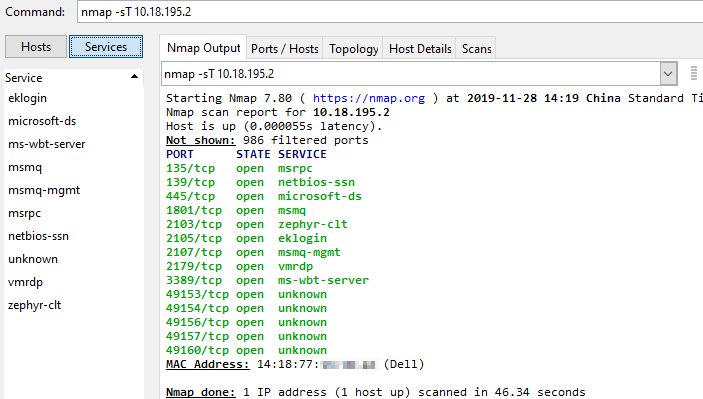


**nmap -sT 目标ip** //TCP connect()扫描，使用完整的三次握手来确定开放的端口

//如果没有指定端口范围，则默认只扫描Nmap定义的常用端口

//在端口时，默认是先进行ping扫描，ping通主机才会进行下一步的

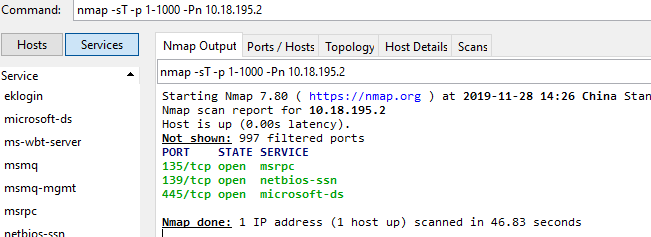
//端口扫描，所以当主机不允许被ping时，端口扫描就不会进行。

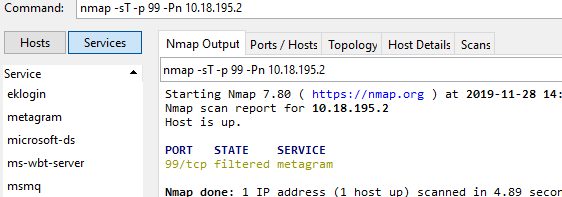


**nmap -sT -p 1-10000 -Pn 目标ip** //-p 指定扫描的端口或端口范围

//-Pn表示不进行ping扫描，不管是否ping得通

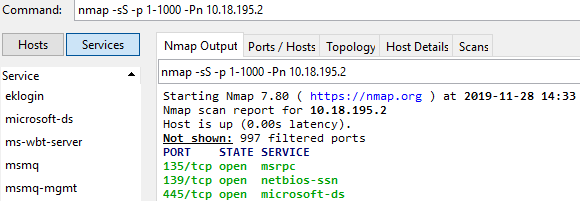
//都会进行端口扫描，也可用-P0表示不ping目标





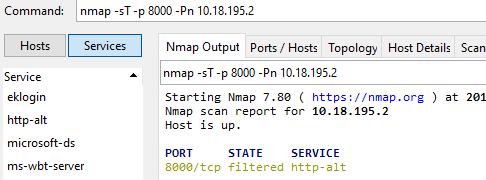
**nmap -sS 目标ip** //SYN半开扫描，只发送syn置位的tcp连接请求包，对方回 //复syn-ack则表示端口有监听，回复rst则不监听，无回复则

//表示被防火墙阻塞了

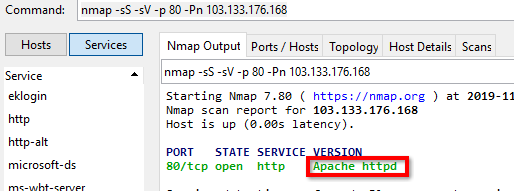


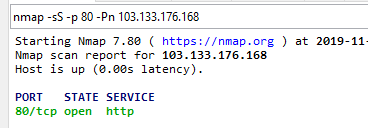
**nmap -sA 目标ip** //ACK扫描，只发送ack置位的tcp确认包，对方有回复rst包

//则说明防火墙没有阻塞此端口，无回复则不清楚是否开放此端口



**nmap -sS -sV -p 80 -Pn 103.133.176.168** //-sV表示探测端口对应的服务和版本



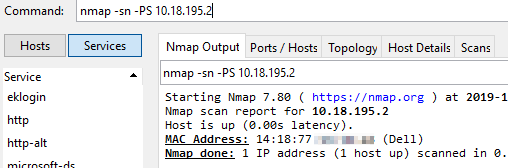


**nmap -sn -PS 10.18.195.2** //-PS表示先用SYN扫描确定主机是否开机，再进行端口

//扫描，此syn扫描只是扫常用的端口号，一旦有一个有回复

//则确定主机开机。若只想确认主机是否开机而不想再扫描其他

//端口，可以使用 -sn参数。

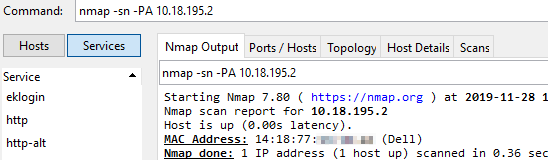


**nmap -sn -PA 10.18.195.2** //-PA表示先用ACK扫描确定主机是否开机，再进行端口

//扫描，此ack扫描只是扫常用的端口号，一旦有一个有回复

//则确定主机开机。若只想确认主机是否开机而不想再扫描其他

//端口，可以使用 -sn参数。

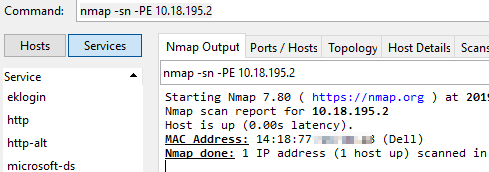


**nmap -sn -PE 10.18.195.2** //-PE表示先用icmp Echo request扫描确定主机是否开机

//再进行端口扫描

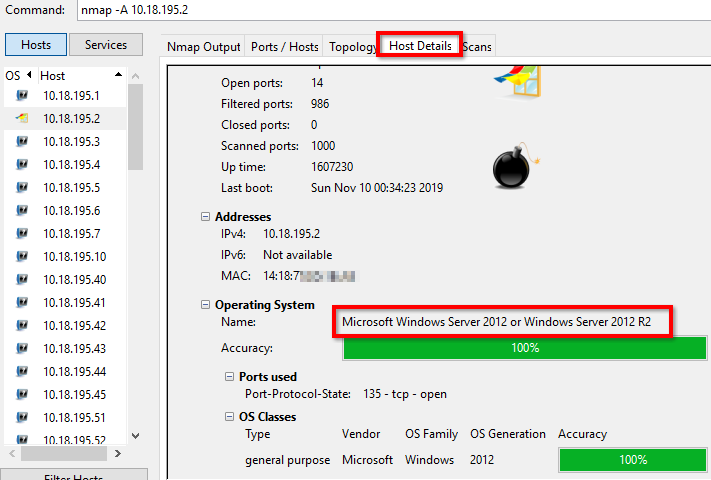
//若只想确认主机是否开机而不想再扫描其他端口，

//可以使用 -sn参数。



**nmap -A 目标ip** //-A表示在端口扫描时获取目标主机的操作系统信息

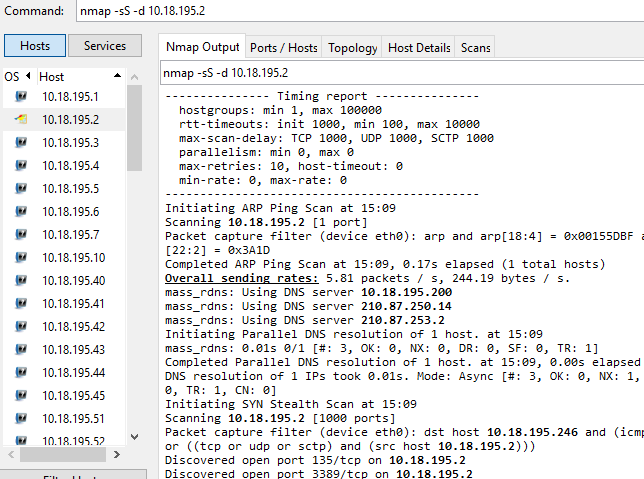
//必须进行端口扫描nmap才能判断出相应的系统信息



nmap -v 目标ip //-v参数表示在扫描过程中显示较为详细的信息

nmap -d 目标ip //-d参数表示在扫描过程中显示最详细的信息

nmap -n 目标ip //-n参数表示在扫描开始前不对目标ip进行dns解析



上图可见一个端口扫描的详细过程为：先进行ping扫描确认主机是否在线，再进行dns解析，再进行端口扫描。

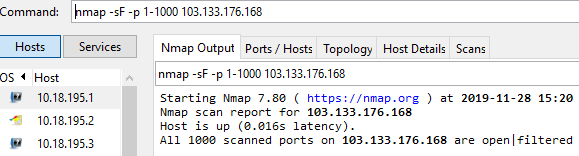
如果我们不想进行ping扫描可以使用-Pn或-P0参数，如果不想进行对目标IP的DNS解析，可以使用-n参数

**其他三个不常用的端口扫描类型**：

snmp -sF 目标ip //FIN扫描（秘密FIN数据包扫描），发送fin置位的tcp数据包，

//响应RST则表示防火墙没有阻塞此端口，但主机上关闭此端口

//无回复则不确定，显示（open|filtered）



snmp -sX 目标ip //XMAS扫描（圣诞树Xmas Tree扫描）发送fin,urg,push置位的

// tcp数据包，有响应则说明开放此端口，无响应则不确定

snmp -sN 目标ip //Null扫描（空扫描），发送没有标志位的tcp数据包

以上三种端口扫描在大多数系统中都没有响应，效果不是很好，一般也不使用。

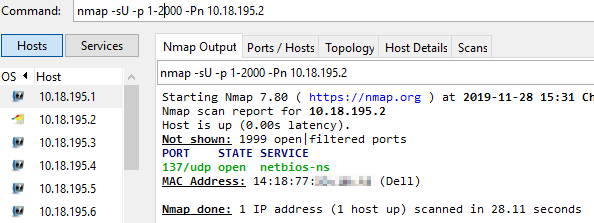
**看到这儿有没有发现什么问题？**

*—— 好像以上的端口扫描全是TCP的，没有UDP的*。

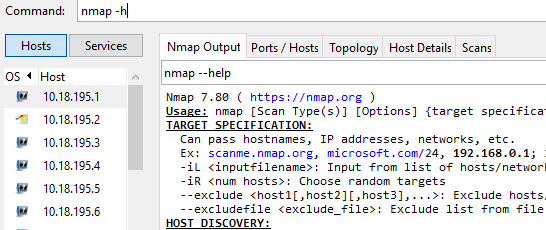
对，默认的扫描都是对TCP端口的扫描，因为udp用得少，但并不代表没有用，所以下面讲一下关于udp的扫描。

UDP的扫描非常慢，因为操作系统对入站的UDP包会有限制，达到若干条，就会阻止一段时间，再允许我们继续发送udp探测包。所以UDP的话一次扫描不要扫太多的端口

**snmp -sU -p 1-2000 目标ip** //-U表示进行UDP端口扫描



其他的参数可以使用命令nmap --help 查看。



**四：总结**

|  |  |  |
| --- | --- | --- |
| **扫描参数** | **释义** | **注意** |
| -h | 查看帮助 |  |
| -V | 查看nmap版本 |  |
| -sP | 只进行Ping扫描，发送icmp echo request包进行探测 |  |
| -sn | 同-sP |  |
| -Pn | 不进行Ping扫描，在端口扫描时默认是先ping的，可以关闭 |  |
| -P0 | 同-Pn |  |
| -F | 快速扫描，缺省的。默认情况下只扫描常用的一些tcp端口 |  |
| -sT | TCP connect()扫描，进行一次完整的tcp连接 | 这6种tcp端口扫描不能同时使用，一次只能用一种 |
| -sS | SYN半开扫描，不完整的tcp连接 |
| -sA | ACK扫描，发送ack置位的包，因为防火墙一般会阻塞syn包入站，而不会阻塞ack包入站 |
| -sF | FIN扫描，发送Fin置位的包 |
| -sX | Xmas扫描，发送Fin,Urg,Push三个标志位置位的包 |
| -sN | NULL扫描，发送不设标志位的tcp包 |
| -PE | 扫描之前先用icmp echo request进行确认主机是否开机 | 这三个扫描，若确认主机开机后默认是会进行端口扫描的。 |
| -PA | 扫描之前先用ACK扫描常用端口进行确认主机是否开机 |
| -PS | 扫描之前先用SYN扫描常用端口进行确认主机是否开机 |
| -sV | 探测端口对应的服务和服务版本 |  |
| -A | 端口扫描时进行探测分析操作系统的信息 |  |
| -p 80  -p 80,81  -p 1-99 | 端口扫描时指定要扫描的 端口或端口范围 |  |
| -sU | 进行UDP端口扫描，可以和TCP端口扫描同时进行 |  |
| -v | 扫描时显示较为详细的信息 |  |
| -d | 扫描时显示最详细的信息 |  |
| -n | 不对主机的ip进行dns解析 |  |
| -oN x.txt | 扫描的结果输出到文件中，文件名为 x.txt |  |

作者：李茂福

2019年11月28日