

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/>



News

- Nmap 7.80 was released for DEFCON 27! [release notes] [download](#)
- Nmap 7.70 is now available! [release notes] | [download](#)
- Nmap turned 20 years old on September 1, 2017! Celebrate by reading the original Phrack #51 article. #Nmap20!
- Nmap 7.60 is now available! [release notes] | [download](#)
- Nmap 7.50 is now available! [release notes] | [download](#)
- Nmap 7 is now available! [release notes] | [download](#)
- We're pleased to release our new and Improved Icons of the Web project—a 5-gigapixel interactive collage of the top million s
- Nmap has been discovered in two new movies! It's used to [hack Matt Damon's brain in Elysium](#) and also to [launch nuclear mis](#)
- We're delighted to announce Nmap 6.40 with 14 new NSE scripts, hundreds of new OS and version detection signatures, and n
- We just released Nmap 6.25 with 85 new NSE scripts, performance improvements, better OS/version detection, and more! [Ar
- Any release as big as Nmap 6 is bound to uncover a few bugs. We've now fixed them with Nmap 6.01!
- Nmap 6 is now available! [release notes] | [download](#)
- The security community has spoken! 3,000 of you shared favorite security tools for our relaunched [SecTools.Org](#). It is sort of l

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。

Microsoft Windows binaries



Please read the [Windows section](#) of the Install Guide for limitations and installation instructions, dependencies and also the Zenmap GUI) or the much smaller command-line zip file version. We also maintain a [guide for users who must run Nmap on earlier Windows releases](#).

Note: The version of Npcap included in our installers may not always be the latest version. If you want to use the latest version, please [install the latest Npcap release](#).

The Nmap executable Windows installer can handle Npcap installation, registry performance improvements, and registry location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows installer.

Latest [stable](#) release self-installer: [nmap-7.80-setup.exe](#)

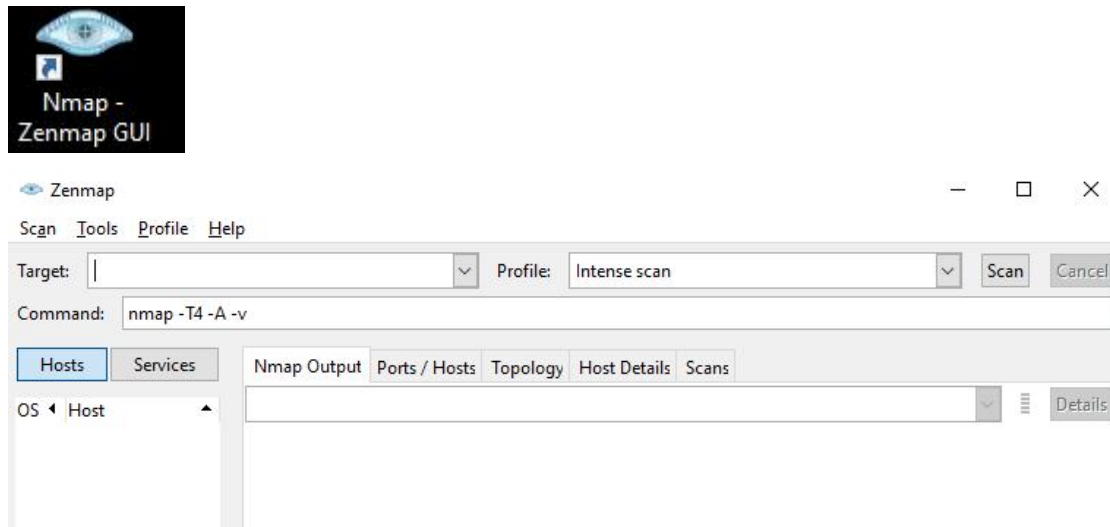
Latest Npcap release self-installer: [npcap-0.9984.exe](#)

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：

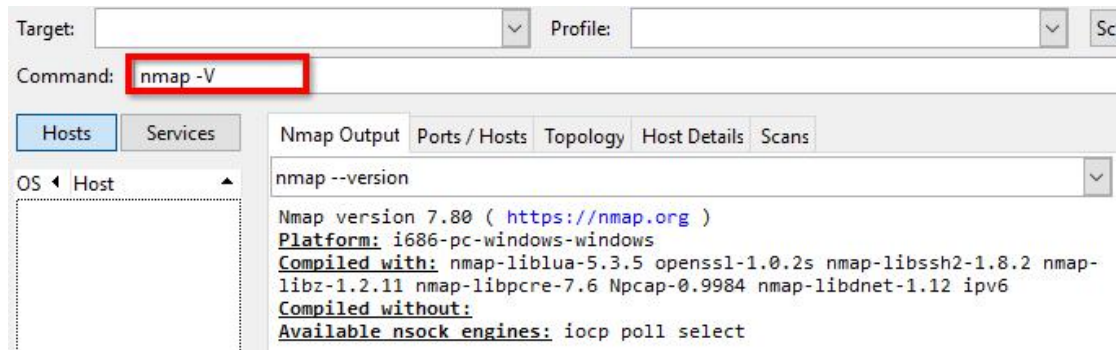
nmap -sS 等扫描参数 目标 ip

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。

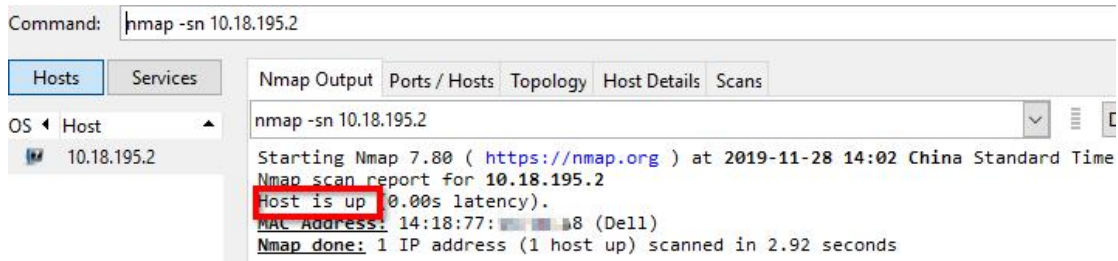
参数可带多个，自由组合，不过有的命令不能同时使用。

三: Nmap 扫描参数

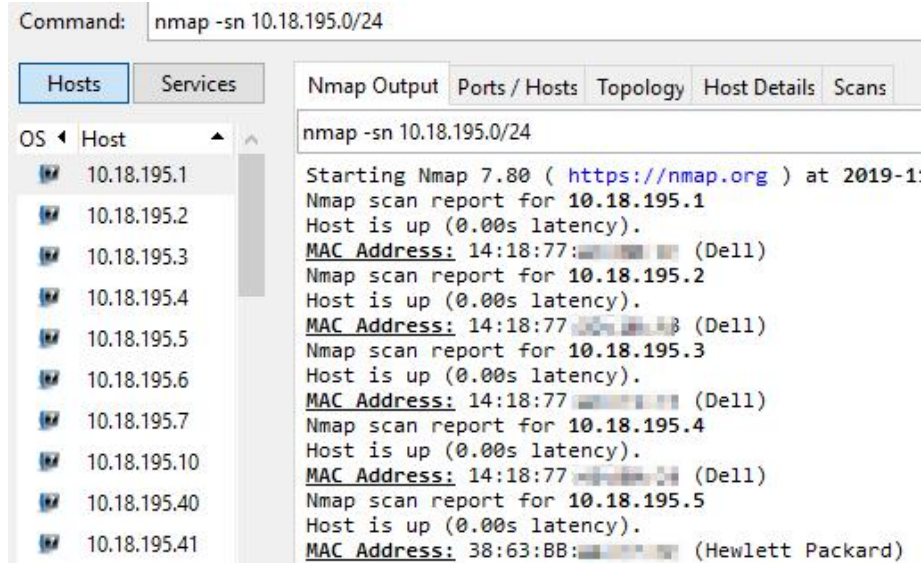
nmap -V //查看 nmap 版本 (大写的 V),也可用 --version



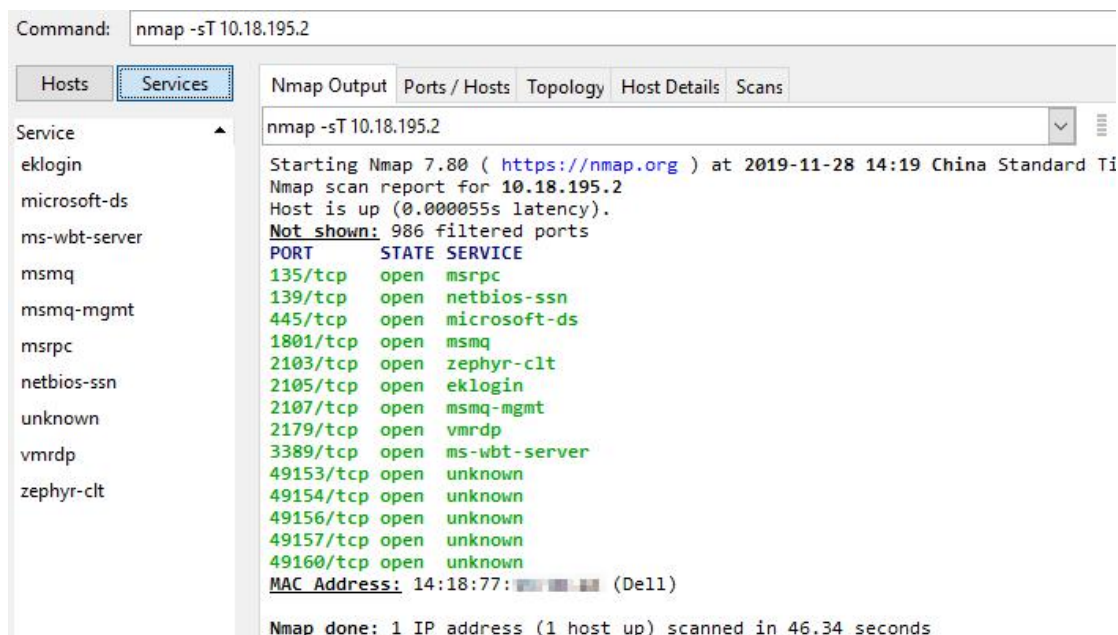
nmap -sP 目标 ip //Ping 扫描, 发送 icmp echo request 确认主机是否开机
//也可用 -sn 表示仅 ping 扫描, 不扫描端口



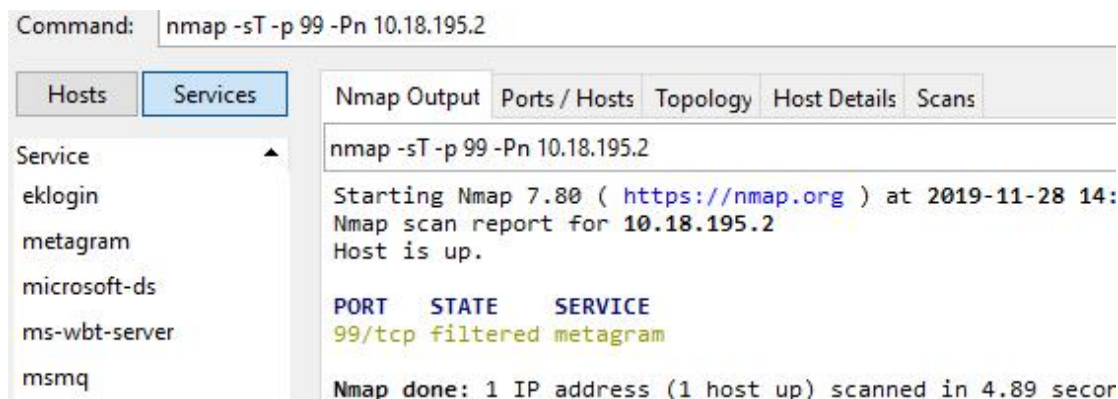
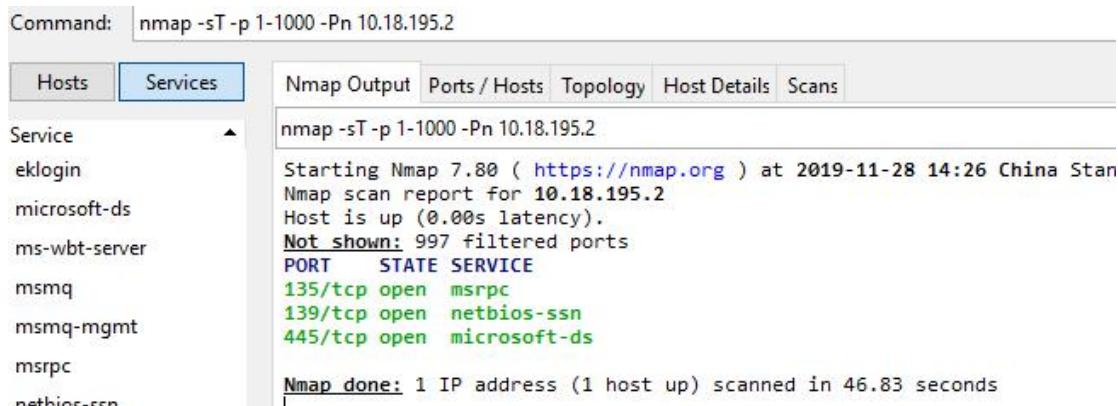
nmap -sn 目标网段/子网掩码位数 //扫描整个网段开机的主机



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

Command: `nmap -sS -p 1-1000 -Pn 10.18.195.2`

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans				
Service	eklogin	<pre> nmap -sS -p 1-1000 -Pn 10.18.195.2 Starting Nmap 7.80 (https://nmap.org) at 2019-11-28 14:33 Nmap scan report for 10.18.195.2 Host is up (0.00s latency). Not shown: 997 filtered ports PORT STATE SERVICE 135/tcp open msrpc 139/tcp open netbios-ssn 445/tcp open microsoft-ds </pre>								

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

Command: `nmap -sT -p 8000 -Pn 10.18.195.2`

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scan				
Service	eklogin	<pre> nmap -sT -p 8000 -Pn 10.18.195.2 Starting Nmap 7.80 (https://nmap.org) at 201 Nmap scan report for 10.18.195.2 Host is up. PORT STATE SERVICE 8000/tcp filtered http-alt </pre>								

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

Command: `nmap -sS -sV -p 80 -Pn 103.133.176.168`

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans				
Service	eklogin	<pre> nmap -sS -sV -p 80 -Pn 103.133.176.168 Starting Nmap 7.80 (https://nmap.org) at 2019-11 Nmap scan report for 103.133.176.168 Host is up (0.00s latency). PORT STATE SERVICE VERSION 80/tcp open http Apache httpd </pre>								

```

nmap -sS -p 80 -Pn 103.133.176.168
Starting Nmap 7.80 ( https://nmap.org ) at 2019-11-
Nmap scan report for 103.133.176.168
Host is up (0.00s latency).

PORT      STATE SERVICE
80/tcp    open  http
  
```

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。

```
Command: nmap -sn -PS 10.18.195.2
```

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
	Service ▲ eklogin http http-alt microsoft-ds	<pre>nmap -sn -PS 10.18.195.2 Starting Nmap 7.80 (https://nmap.org) at 2019-11-28 11:00:00 Nmap scan report for 10.18.195.2 Host is up (0.00s latency). MAC Address: 14:18:77:00:00:00 (Dell) Nmap done: 1 IP address (1 host up) scanned in 0.00s</pre>				

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。

```
Command: nmap -sn -PA 10.18.195.2
```

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
	Service ▲ eklogin http http-alt	<pre>nmap -sn -PA 10.18.195.2 Starting Nmap 7.80 (https://nmap.org) at 2019-11-28 11:00:00 Nmap scan report for 10.18.195.2 Host is up (0.00s latency). MAC Address: 14:18:77:00:00:00 (Dell) Nmap done: 1 IP address (1 host up) scanned in 0.36 sec</pre>				

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。

```
Command: nmap -sn -PE 10.18.195.2
```

Hosts	Services	Nmap Output	Ports / Hosts	Topology	Host Details	Scans
	Service ▲ eklogin http http-alt microsoft-ds	<pre>nmap -sn -PE 10.18.195.2 Starting Nmap 7.80 (https://nmap.org) at 2019-11-28 11:00:00 Nmap scan report for 10.18.195.2 Host is up (0.00s latency). MAC Address: 14:18:77:00:00:00 (Dell) Nmap done: 1 IP address (1 host up) scanned in 0.00s</pre>				

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

Command: nmap -A 10.18.195.2

Hosts Services Nmap Output Ports / Hosts Topology **Host Details** Scans

OS Host

- 10.18.195.1
- 10.18.195.2
- 10.18.195.3
- 10.18.195.4
- 10.18.195.5
- 10.18.195.6
- 10.18.195.7
- 10.18.195.10
- 10.18.195.40
- 10.18.195.41
- 10.18.195.42
- 10.18.195.43
- 10.18.195.44
- 10.18.195.45
- 10.18.195.51
- 10.18.195.52

Open ports: 14
Filtered ports: 986
Closed ports: 0
Scanned ports: 1000
Up time: 1607230
Last boot: Sun Nov 10 00:34:23 2019

Addresses
IPv4: 10.18.195.2
IPv6: Not available
MAC: 14:18:7...

Operating System
Name: Microsoft Windows Server 2012 or Windows Server 2012 R2
Accuracy: 100%

Ports used
Port-Protocol-State: 135 - tcp - open

OS Classes

Type	Vendor	OS Family	OS Generation	Accuracy
general purpose	Microsoft	Windows	2012	100%

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

Command: nmap -sS -d 10.18.195.2

Hosts Services Nmap Output Ports / Hosts Topology Host Details Scans

OS Host

- 10.18.195.1
- 10.18.195.2
- 10.18.195.3
- 10.18.195.4
- 10.18.195.5
- 10.18.195.6
- 10.18.195.7
- 10.18.195.10
- 10.18.195.40
- 10.18.195.41
- 10.18.195.42
- 10.18.195.43
- 10.18.195.44
- 10.18.195.45
- 10.18.195.51
- 10.18.195.52

nmap -sS -d 10.18.195.2

----- Timing report -----
hostgroups: min 1, max 100000
rtt-timeouts: init 1000, min 100, max 10000
max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
parallelism: min 0, max 0
max-retries: 10, host-timeout: 0
min-rate: 0, max-rate: 0

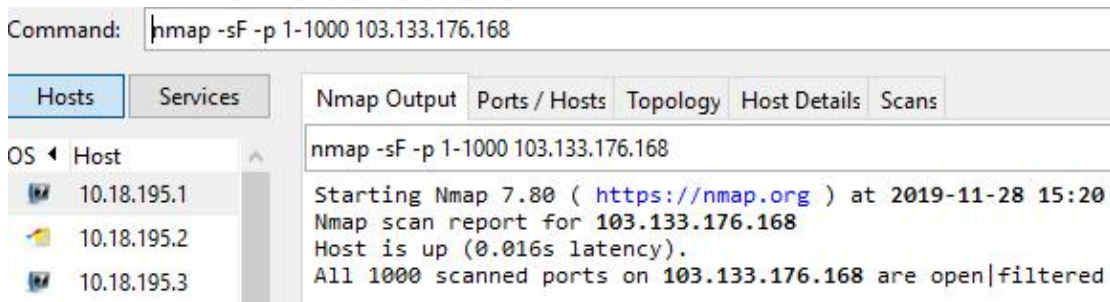
Initiating ARP Ping Scan at 15:09
Scanning 10.18.195.2 [1 port]
Packet capture filter (device eth0): arp and arp[18:4] = 0x00155DBF ;
[22:2] = 0x3A1D
Completed ARP Ping Scan at 15:09, 0.17s elapsed (1 total hosts)
Overall sending rates: 5.81 packets / s, 244.19 bytes / s.
mass_rdns: Using DNS server 10.18.195.200
mass_rdns: Using DNS server 210.87.250.14
mass_rdns: Using DNS server 210.87.253.2
Initiating Parallel DNS resolution of 1 host. at 15:09
mass_rdns: 0.01s 0/1 [#: 3, OK: 0, NX: 0, DR: 0, SF: 0, TR: 1]
Completed Parallel DNS resolution of 1 host. at 15:09, 0.00s elapsed
DNS resolution of 1 IPs took 0.01s. Mode: Async [#: 3, OK: 0, NX: 1,
0, TR: 1, CN: 0]
Initiating SYN Stealth Scan at 15:09
Scanning 10.18.195.2 [1000 ports]
Packet capture filter (device eth0): dst host 10.18.195.246 and (icmp
or ((tcp or udp or sctp) and (src host 10.18.195.2)))
Discovered open port 135/tcp on 10.18.195.2
Discovered open port 3389/tcp on 10.18.195.2

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 -PO 参数， 如果想不想进行对目标 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。

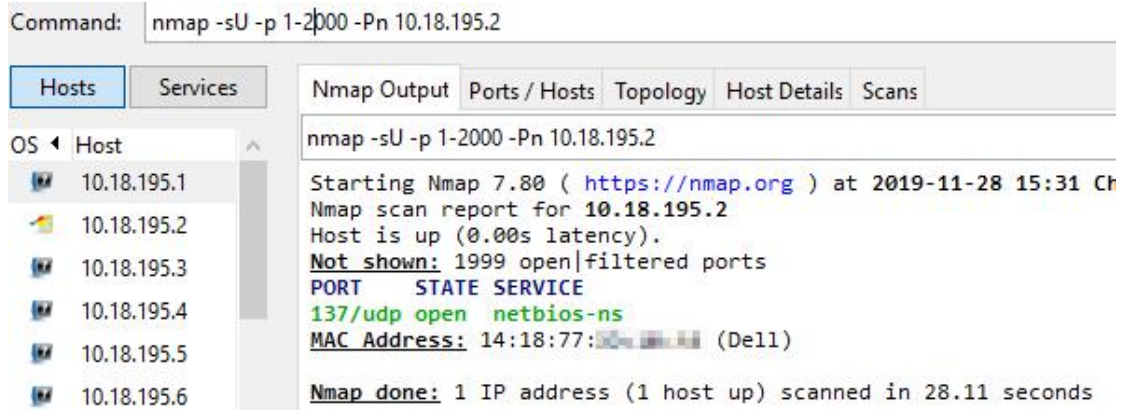
看到这儿有没有发现什么问题？

—— 好像以上的端口扫描全是 TCP 的，没有 UDP 的。

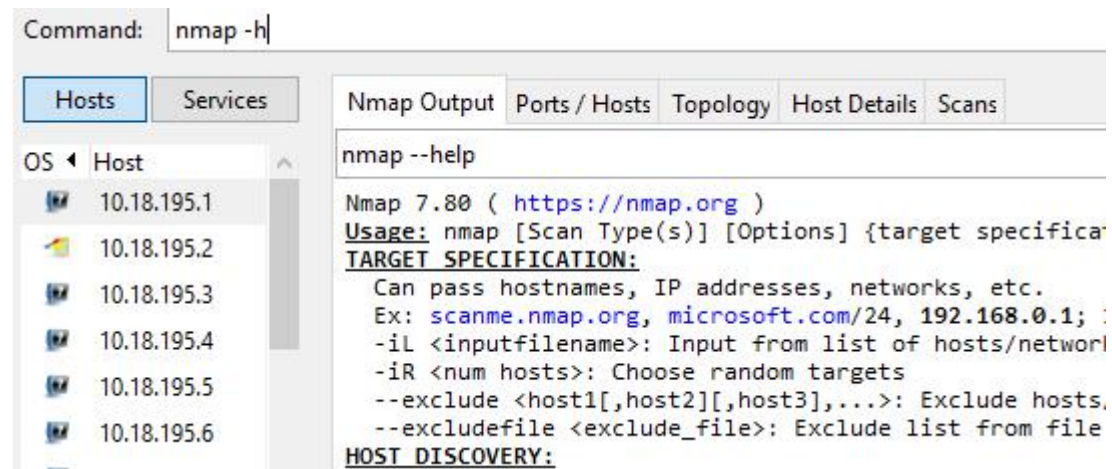
对，默认的扫描都是对 TCP 端口的扫描，因为 udp 用得少，但并不代表没有用，所以下面讲一下关于 udp 的扫描。

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。



The screenshot shows the Nmap GUI interface. At the top, the command field contains `nmap -h`. Below this, there are two tabs: "Hosts" and "Services". The "Hosts" tab is active, displaying a list of hosts with their IP addresses: 10.18.195.1, 10.18.195.2, 10.18.195.3, 10.18.195.4, 10.18.195.5, and 10.18.195.6. To the right of the host list, there are four sub-tabs: "Nmap Output", "Ports / Hosts", "Topology", "Host Details", and "Scans". The "Nmap Output" sub-tab is active, showing the help text for the `nmap --help` command. The help text includes the version (7.80), usage instructions, target specification options, and a section for host discovery.

```
Command: nmap -h
```

Hosts Services

OS Host

- 10.18.195.1
- 10.18.195.2
- 10.18.195.3
- 10.18.195.4
- 10.18.195.5
- 10.18.195.6

Nmap Output Ports / Hosts Topology Host Details Scans

```
nmap --help

Nmap 7.80 ( https://nmap.org )
Usage: nmap [Scan Type(s)] [Options] {target specification}
TARGET SPECIFICATION:
  Can pass hostnames, IP addresses, networks, etc.
  Ex: scanme.nmap.org, microsoft.com/24, 192.168.0.1; :
  -iL <inputfilename>: Input from list of hosts/networks
  -iR <num hosts>: Choose random targets
  --exclude <host1[,host2][,host3],...>: Exclude hosts.
  --excludefile <exclude_file>: Exclude list from file
HOST DISCOVERY:
```

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	
-PO	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，一次只能使用一种
-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