链滴

Linux 命令 -nmap

作者：james

原文链接：https://ld246.com/article/1484718532202

来源网站：链滴

● 主机扫描工具nmap

1. 进行ping扫描，打印出对扫描做出响应的主机,不做进一步测试(如端口扫描或者操作系统探测)：nmap -sP 192.168.1.0/24

```
james@james:~ > nmap -sP 192.168.179.0/24

Starting Nmap 6.40 ( http://nmap.org ) at 2017-01-12 16:23 CST
Nmap scan report for 192.168.179.1
Host is up (0.00061s latency).
Nmap scan report for 192.168.179.2
Host is up (0.00042s latency).
Nmap scan report for localhost (192.168.179.132)
Host is up (0.000032s latency).
Nmap scan report for localhost (192.168.179.133)
Host is up (0.00041s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 2.41 seconds
```

2. 探测目标主机开放的端口，可以指定一个以逗号分隔的端口列表(如-PS22，23，25，80)：nmap -S 192.168.1.234

```
james@james:~ > nmap -PS 192.168.179.2

Starting Nmap 6.40 ( http://nmap.org ) at 2017-01-12 16:24 CST
Nmap scan report for 192.168.179.2
Host is up (0.00049s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain

Nmap done: 1 IP address (1 host up) scanned in 0.06 seconds
```

3. 确定目标机支持哪些IP协议 (TCP，ICMP，IGMP等):nmap -sO 192.168.1.19

```
james@james:~ > nmap -sO 192.168.179.2
You requested a scan type which requires root privileges.
QUITTING!
james@james:~ > sudo nmap -sO 192.168.179.2
[sudo] password for james:

Starting Nmap 6.40 ( http://nmap.org ) at 2017-01-12 16:24 CST
Nmap scan report for 192.168.179.2
Host is up (0.089s latency).
Not shown: 252 closed protocols
PROTOCOL STATE         SERVICE
1        open          icmp
6        open          tcp
17       open|filtered udp
47       open|filtered gre
MAC Address: 00:50:56:F9:0E:1E (VMware)

Nmap done: 1 IP address (1 host up) scanned in 3.07 seconds
```

4. 探测目标主机的操作系统：

● nmap -O 192.168.1.19

```
james@james:~ > sudo nmap -O 192.168.179.2

Starting Nmap 6.40 ( http://nmap.org ) at 2017-01-12 16:30 CST
Nmap scan report for 192.168.179.2
Host is up (0.010s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
53/tcp open  domain
MAC Address: 00:50:56:F9:0E:1E (VMware)
Aggressive OS guesses: Microsoft Windows 7 Enterprise (93%), Microsoft Windows XP SP3 (9
%), DD-WRT v24-sp2 (Linux 2.4.37) (91%), DVTel DVT-9540DW network camera (90%), Linux 3
2 (90%), BlueArc Titan 2100 NAS device (89%), Brother HL-5170DN printer (87%), Pirelli DP-10
VoIP phone (87%), Aethra Starvoice 1042 ADSL router (87%), Brother HL-1870N printer (87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 8.15 seconds
```

● nmap -A 192.168.1.19

```
james@james:~ > sudo nmap -A 192.168.179.2

Starting Nmap 6.40 ( http://nmap.org ) at 2017-01-12 16:30 CST
Nmap scan report for localhost (192.168.179.2)
Host is up (0.00036s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE VERSION
53/tcp open  domain  Microsoft DNS
| dns-nsid:
|_  bind.version: I do not know
MAC Address: 00:50:56:F9:0E:1E (VMware)
Aggressive OS guesses: Microsoft Windows 7 Enterprise (93%), Microsoft Windows XP SP3 (9
%), DVTel DVT-9540DW network camera (91%), DD-WRT v24-sp2 (Linux 2.4.37) (90%), Linux 3
2 (90%), BlueArc Titan 2100 NAS device (89%), Brother HL-5170DN printer (88%), Aethra Star
oice 1042 ADSL router (87%), Brother HL-1870N printer (87%), Brother NC-3100h print server
87%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

TRACEROUTE
HOP RTT     ADDRESS
1   0.37 ms localhost (192.168.179.2)

OS and Service detection performed. Please report any incorrect results at http://nmap.org/s
bmit/ .
Nmap done: 1 IP address (1 host up) scanned in 19.32 seconds
```

原文链接：Linux 命令 -nmap