Nmap扫描基础常用命令

1、扫描单个目标

nmap ip

```
如：nmap 192.168.0.101
```

2、扫描多个目标

nmap ip1 ip2 适用于目标地址不再同一个网段或在同一网段不连续且数量不多的情况。

```
如：nmap 192.168.0.101 192.168.0.110
```

3、扫描一个范围内的目标

nmap xxx.xxx.xxx.xxx-xxx

```
如：nmap 192.168.0.100·110
```

4、扫描目标地址所在某网段

namp xxx.xxx.xxx.xxx/xx

```
如：nmap 192.168.0.1/24
```

5、扫描包含主机列表的文件中的所有地址

nmap -iL

```
如：nmap -iL /root/target.txt
```

6、扫描除了一个目标地址之外的所有地址

nmap ip段 -exclude 被排除的ip

```
如：nmap 192.168.0.100-110 -exclude 192.168.0.103
   nmap 192.168.0.1/24 -exclude 192.168.0.103
```

7、扫描除了某一个文件中的地址之外的所有地址

nmap ip段 -excludefile

```
如：nmap 192.168.0.100-110 -excludefile /root/targets.txt
   nmap 192.168.0.1/24 -excludefile /root/targets.txt
```

8、扫描目标地址的指定端口

nmap ip -p 端口1，端口2，端口3.....

```
如:nmap 192.168.0.101 -p 80,8080,3306,3389
```

9、对目标地址进行路由跟踪

nmap --traceroute ip

```
如：nmap --traceroute 192.168.0.101
```

10、扫描目标地址**C**段的在线主机

nmap -sP ip段

```
如：nmap -sP 192.168.0.1/24
```

11、扫描目标地址进行操作系统版本

nmap -O ip

```
如：nmap -O 192.168.0.101
```

12、扫描目标地址开放服务**(**端口**)**版本

nmap -sV ip

```
如：nmap -sV 192.168.0.101
```

13、探测防火墙

nmap -sF -T4 ip

```
如：nmap -sF -T4 192.168.0.101
```

14、**Nmap** 全端口扫描命令是什么

nmap -p- ip

```
如：nmap -p1-65535 192.168.0.101  nmap -p- 192.168.0.101
```

进阶用法**-advanced**

nmap --script=xx 使用某个脚本进行扫描

1、弱口令扫描

nmap --script=auth ip 对某个主机或某网段主机的应用进行弱口令检测

```
如：nmap --script=auth 192.168.0.101
```

2、暴力破解

nmap --script=brute ip 可以对胡句酷、MB、SNMP等进行简单的暴力破解

```
如：nmap --script=brute 192.168.0.101
```

3、扫描常见漏洞

nmap --script=vuln ip

```
如：nmap --script=vuln 192.168.0.101
```

4、使用脚本进行应用服务扫描

nmap --script=xxx ip 对常见应用服务进行扫描 如：VNC、MySQL、Telnet、Rync等服务

```
如VNC服务：nmap --script=realvnc-auth-bypass 192.168.0.101
```

5、探测局域网内服务开放情况

nmap -n -p xxx --script=broadcast ip

```
如：nmap --script=broadcast 192.168.0.101
```

6、**Whois**解析

nmap -script external url

```
如：nmap -script external baidu.com
```