nmap

网络探测和安全审核

补充说明

nmap命令 是一款开放源代码的网络探测和安全审核工具，它的设计目标是快速地扫描大型网络。

语法

```
nmap(选项)(参数)
```

选项

```
-O□激活操作探测；
-P0□值进行扫描，不ping主机；
-PT□是同TCP的ping□
-sV□探测服务版本信息；
-sP□ping扫描，仅发现目标主机是否存活；
-ps□发送同步□SYN□报文；
-PU□发送udp ping□
-PE□强制执行直接的ICMPping□
-PB□默认模式，可以使用ICMPping和TCPping□
-6：使用IPv6地址；
-v□得到更多选项信息；
-d□增加调试信息地输出；
-oN□以人们可阅读的格式输出；
-oX□以xml格式向指定文件输出信息；
-oM□以机器可阅读的格式输出；
-A□使用所有高级扫描选项；
--resume□继续上次执行完的扫描；
-P□指定要扫描的端口，可以是一个单独的端口，用逗号隔开多个端口，使用“ - ”表示端口范围；
-e□在多网络接口Linux系统中，指定扫描使用的网络接口；
-g□将指定的端口作为源端口进行扫描；
--ttl□指定发送的扫描报文的生存期；
--packet-trace□显示扫描过程中收发报文统计；
--scanflags□设置在扫描报文中的TCP标志。
--send-eth/--send-ip 使用原始以太网发送/构造指定IP发送
```

参数

ip地址：指定待扫描报文中的TCP地址。

实例

安装nmap

```
yum install nmap
```

使用nmap扫描www.jsdig.com的开放端口

```
[root@localhost ~]# nmap www.jsdig.com

Starting Nmap 4.11 ( http://www.insecure.org/nmap/ ) at 2013-12-28 00:06 CST
Interesting ports on 100-42-212-8.static.webnx.com (100.42.212.8):
Not shown: 1678 filtered ports
PORT   STATE service
22/tcp open  ssh
80/tcp open  http

Nmap finished: 1 IP address (1 host up) scanned in 45.870 seconds
```