Masscan

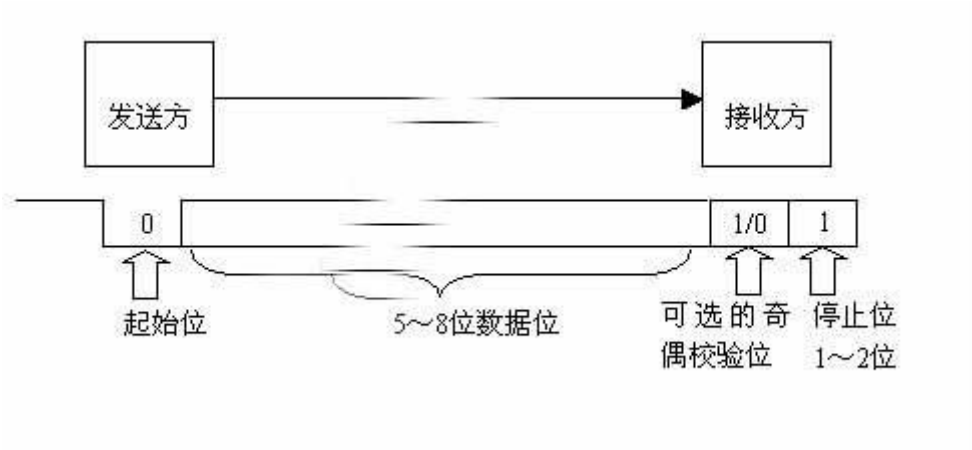
Massca是一个海量IP端口扫描协议，这也是最快的互联网端口扫描工具。他可以扫描整个互联网，不到六分钟的时间，他可可以传输1000万个数据包。他产生的结果类似于著名的端口扫描工具Nmap。

在速度方面，Masscau有着非常明显的有是，他的内部与Scanrand、Unicornscan和Zmap。因为他使用的是异步传输，所以比他们更快于其他扫描仪。

除此之外，Masscan更加的灵活，你甚至可以使用Masscan扫描任何一个地址，并且他还支持一个扫描端口的范围。

——*Robert David Graham*

一，什么是异步传输（Asynchronous Transmission）



异步传输也叫“信息元中继”，可以将比特分成一个一个小组进行传输，小组可以是八位数也可以是一个字符甚至更长。发送方可以在任何时候向对方发送数据包，但接受方不会知道在什么时候到达。

二，帮助手册

```
MASSCAN是一种快速端口扫描仪。主要输入参数是要扫描的IP地址/范围以及端口号。下面是一个示例，它
扫描10.x.x.x网络以查找web服务器：

masscan 10.0.0.0/8 -p80



程序自动检测网络接口/适配器设置。如果这个
如果失败，则必须手动设置。以下是需要的所有参数示例：

--adapter-ip 192.168.10.123
```

```
--adapter-mac 00-11-22-33-44-55
--router-mac 66-55-44-33-22-11
```

可以通过命令行或配置文件设置参数。两个名字都一样。因此，上述适配器设置将在配置文件中显示如下：

```
adapter-ip = 192.168.10.123
adapter-mac = 00-11-22-33-44-55
router-mac = 66-55-44-33-22-11
```

所有单破折号参数都有一个拼写的双破折号等效值，所以“-p80”与配置文件中的“--ports 80”（或“ports=80”）相同。要使用配置文件，请键入：

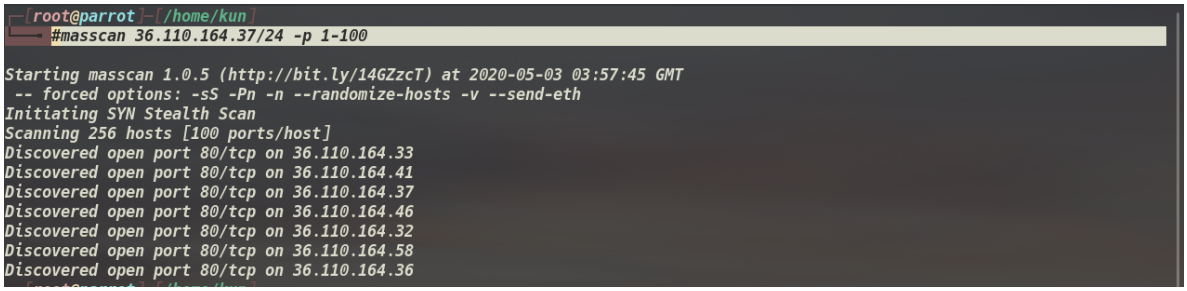
```
masscan -c <filename>
```

要从当前设置生成配置文件，请使用--echo选项。这会阻止程序实际运行，而只是回显当前配置。这是生成第一个配置文件或查看未知参数列表的有用方法关于。我建议你现在就试试：

```
masscan -p1234 --echo
```

```
MASSCAN is a fast port scanner. The primary input parameters are the
IP addresses/ranges you want to scan, and the port numbers. An example
is the following, which scans the 10.x.x.x network for web servers:
 masscan 10.0.0.0/8 -p80
The program auto-detects network interface/adapter settings. If this
fails, you'll have to set these manually. The following is an
example of all the parameters that are needed:
 --adapter-ip 192.168.10.123
 --adapter-mac 00-11-22-33-44-55
 --router-mac 66-55-44-33-22-11
Parameters can be set either via the command-line or config-file. The
names are the same for both. Thus, the above adapter settings would
appear as follows in a configuration file:
 adapter-ip = 192.168.10.123
 adapter-mac = 00-11-22-33-44-55
 router-mac = 66-55-44-33-22-11
All single-dash parameters have a spelled out double-dash equivalent,
so '-p80' is the same as '--ports 80' (or 'ports = 80' in config file).
To use the config file, type:
 masscan -c <filename>
To generate a config-file from the current settings, use the --echo
option. This stops the program from actually running, and just echoes
the current configuration instead. This is a useful way to generate
your first config file, or see a list of parameters you didn't know
about. I suggest you try it now:
 masscan -p1234 --echo
```

三，命令实例



masscan 16.110.164.37/24 -p 1-100

扫描目标1 ~ 100内所开放的端口

> 当然你也可以针对一个端口进行扫描，比如：
>
> masscan xx.xx.xxx.x/24 -p 80

四，无法访问错误解决方案

如果你无法对目标进行检索的话，那么你需要使用以下流程进行修改：

查看配置文件

```
masscan --echo
```

配置IP、MAC、路由器等

```
adapter-ip = 192.168.10.123     // 适配器IP

adapter-mac = 00-11-22-33-44-55 // 适配器MAC

router-mac = 66-55-44-33-22-11  // 路由器MAC
```

使用配置文件

```
masscan -c 文件名
```

生成配置文件

```
masscan -p1234 --echo
```

五，附加

Masscan除了支持自己特有的语法外，还支持Nmap的绝大部分语法，你可以使用以下命令进行查看：

```
masscan --nmap
```