MASSCAN 是一个快速端口扫描程序. 他的主要输入参数是

您要扫描的IP地址/范围, 和端口号码. 一个例子

以下是扫描10 Web服务器10.x.x.x网络:

masscan 10.0.0.0/8 -p80

该程序自动检测网络接口/适配器设置。 如果自动配置失败，则必须手动配置。

例如

--适配器的IP 地址192.168.10.123

--适配器的MAC地址 00-11-22-33-44-55

--路由器的MAC地址 66-55-44-33-22-11

参数可以通过命令行或配置文件设置. 如果两个文件的名字相同. 因此, 上面的适配器设置将在配置文件中出现如下:

--适配器的IP 地址192.168.10.123

--适配器的MAC地址 00-11-22-33-44-55

--路由器的MAC地址 66-55-44-33-22-11

所有的single-dash 参数 有一个输出等效的 double-dash

所以'-p80' 就像 '--ports 80' 一样(or 'ports = 80' 在配置文件).

要使用配置文件，类型：

masscan -c <filename>

从当前设置生成配置文件,使用 --echo

选项.这阻止了程序的实际运行，只有echos而不是当前的配置. 这是一个有用的方法来生成

您的第一个配置文件, 或看到一个参数列表，你不知道

关于。我建议你现在试试：

masscan -p1234 --echo

用法:

masscan -p80,8000-8100 10.0.0.0/8 --rate=10000

用10kpps的速度扫描在10.X.X.X 下扫描一些网络端口

masscan --nmap

列出这些选项是兼容的实现

masscan -p80 10.0.0.0/8 --banners -oB <filename>

将扫描二进制格式的结果保存到<文件名>

masscan --open --banners --readscan <filename> -oX <savefile>

读二进制扫描结果<文件名>并将其保存为XML文件> <