监测服务器端口是否被扫描

端口扫描方式有很多种，`SYN`扫描是最常见的扫描方式，也称为半连接扫描或半开放扫描。这种扫描方式具有很多优点。比如，性能表现好，每秒钟可以扫描上千个端口。扫描较为隐蔽，不易被发现，因为它从来不会完成`TCP`连接，而服务器的守护进程一般不会记录这种没有完成的连接。我现在所介绍的是，如何监测`SYN`扫描，哪些端口被扫描了，以及是谁在扫描。

一、查看被扫描的端口及扫描者IP

后台监控`tcp`连接，并保存文件：

```
nohup tcpdump -n "tcp[tcpflags] == tcp-syn" 2>&1 > syn.scan &
或
nohup tcpdump -n "tcp[13] == 2" 2>&1 > syn.scan &
```

> 使用`tcpdump`抓取`tcp`标志位为`SYN`的数据包，并将结果保存在文件`syn.scan`中。

查看被扫描的端口及其排名：

```
awk -F '[ .:]' '{print $16}' syn.scan | sort | uniq -c | sort -n
```

> 通过`awk`提取端口，并对其排序，去重并计数，对次数进行排序。

查看扫描者`IP`及扫描次数：

```
awk -F '[ .]' '{print $4"."$5"."$6"."$7}' syn.scan | sort | uniq -c |sort -n
```

> 通过`awk`提取发送`SYN`数据包的`IP`，并对其进行排序，去重并计数，对次数进行排序。

二、统计扫描者位置信息

我们已经知道了扫描者的`IP`，现在来统计下他们都来自哪里。看看这些扫描者都来自哪些国家，来自哪些城市。

提取扫描者`IP`并保存为文件：

```
awk -F '[ .]' '{print $4"."$5"."$6"."$7}' syn.scan | sort | uniq > ip.list
```

> 通过`awk`提取发送`SYN`数据包的`IP`，并对其进行排序去重，将结果保存在文件。

我们需要用一个小脚本来获取IP详细信息：

此次使用的`IP`数据库为`ipinfo.io`，注册后每月可免费查询五万次，不注册每日可查询一千次。

新建一个小脚本`lookup.sh`来获取IP信息：

```
#!/bin/bash

while read LINE
do
        curl ipinfo.io/$LINE?token=1d9916617400c6
done < ip.list
```

将获取到的信息保存为文件：

```
./lookup.sh > ip.info
```

查看扫描者国家信息及其排名：

```
grep country ip.info | sort | uniq -c | sort -n
```

查看扫描者城市信息及其排名：

```
grep city ip.info | sort | uniq -c | sort -n
```