**nmap编写脚本**

nmap编写脚本时得到的总结：

这使用自己编写的脚本出现错误的适合可以使用-debug进行调试

例如:

nmap -sV --script=demo -d 127.0.0.1 -> 会给出详细的报错信息

nmap API手册大全：

<https://nmap.org/nsedoc/lib/>

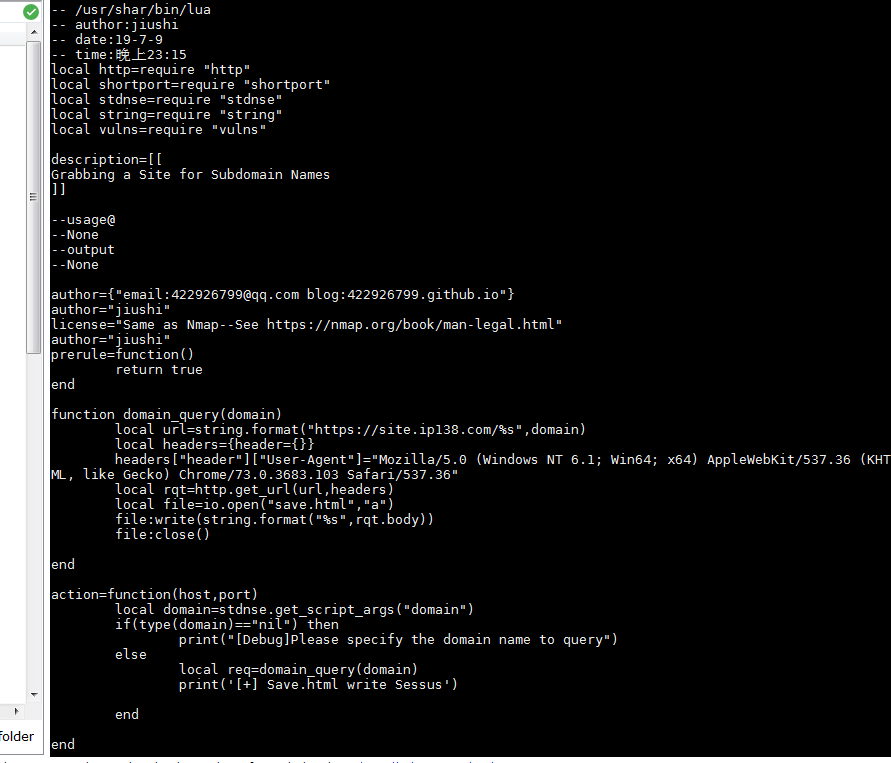
Nmap编写自定义脚本的规则：

<https://nmap.org/book/nse-script-format.html>

[https://nmap.org/book/nse-tutorial.html#nse-tutorial-rule](https://nmap.org/book/nse-tutorial.html" \l "nse-tutorial-rule)

一个小例子：

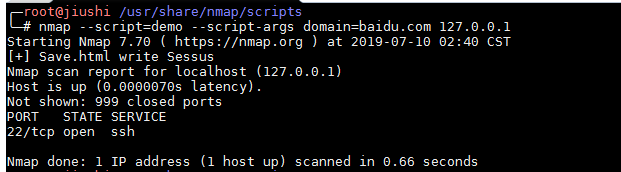
抓取site138.com指定子域名的信息进行保存

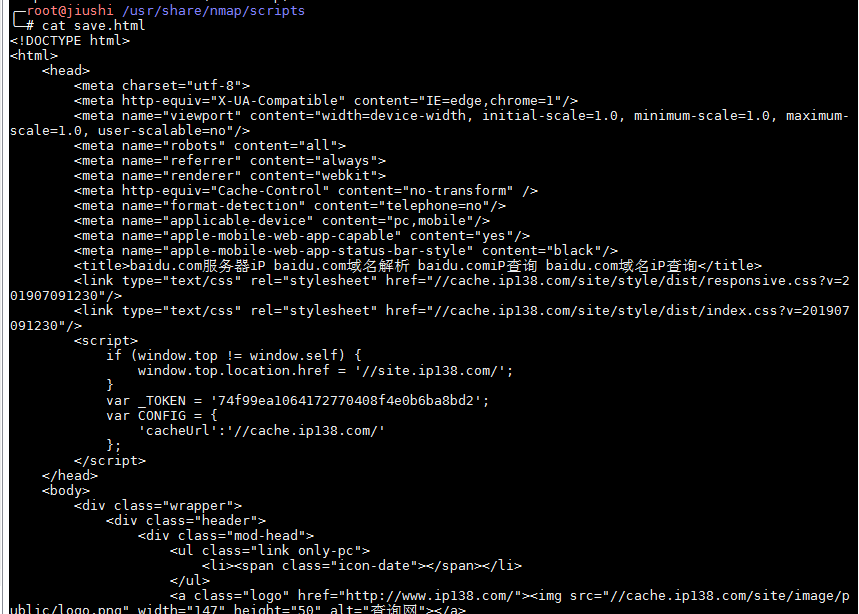


源码：

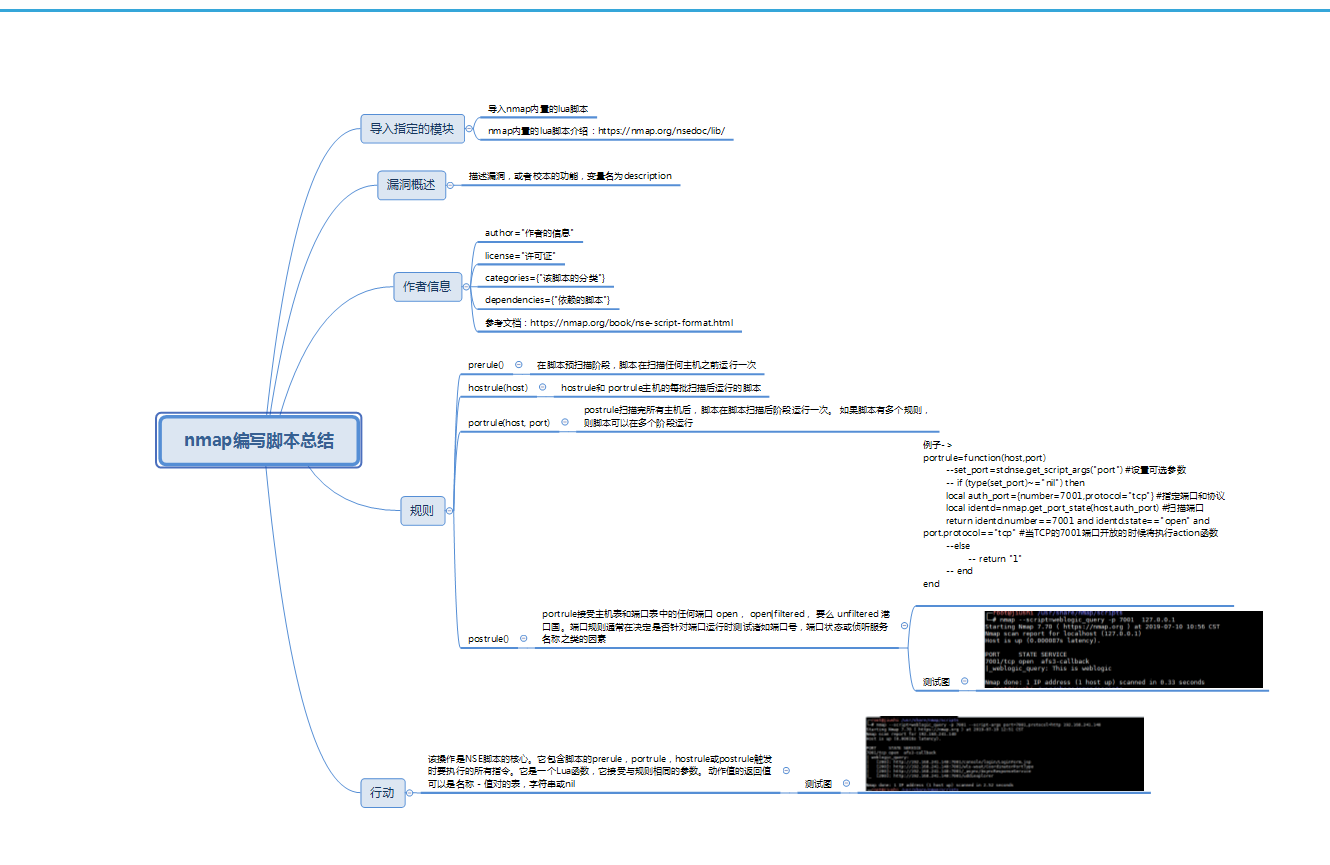


测试结果：





总结成的流程图



源代码例子：



实战测试结果

