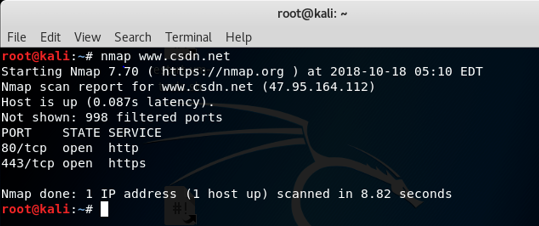
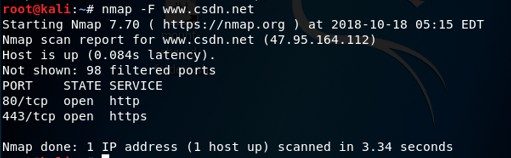
**渗透测试笔记**

1. **利用Nmap扫描网站服务器的端口开放情况**

首先打开Kali终端，输入nmap www.csdn.net，如图：

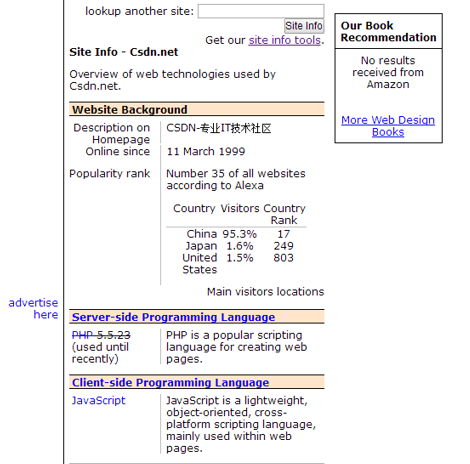


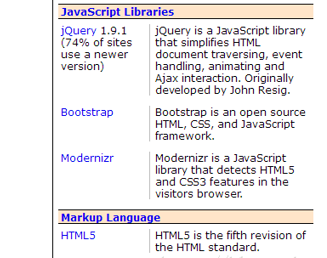
通过这个结果可以表明csdn上的端口开放了80端口以及443端口，这两个端口都十分重要，因为80端口适用于给用户呈现出数据，给用户看网站用的，443端口也是一个比较重要的端口。而且此网站并没有其他端口的开放，说明安全性还是很好的。  
  
**二、利用curl工具嗅探服务器的后台操作系统以及前端后台语言种类**



能够扫描前端的语言为html 。

打开链接 https://w3techs.com/sites 进行在线测试,结果如下：





我们可以清晰的看到，csdn的前端框架是jquery，一种在几年前流行的前端框架，但是做出来网页效果却异常华丽。以及Bootstrap，一种十分简单的框架。后台则使用了php语言，一种落后但十分简单易学的语言作为后台框架，作为一种不错的选择。