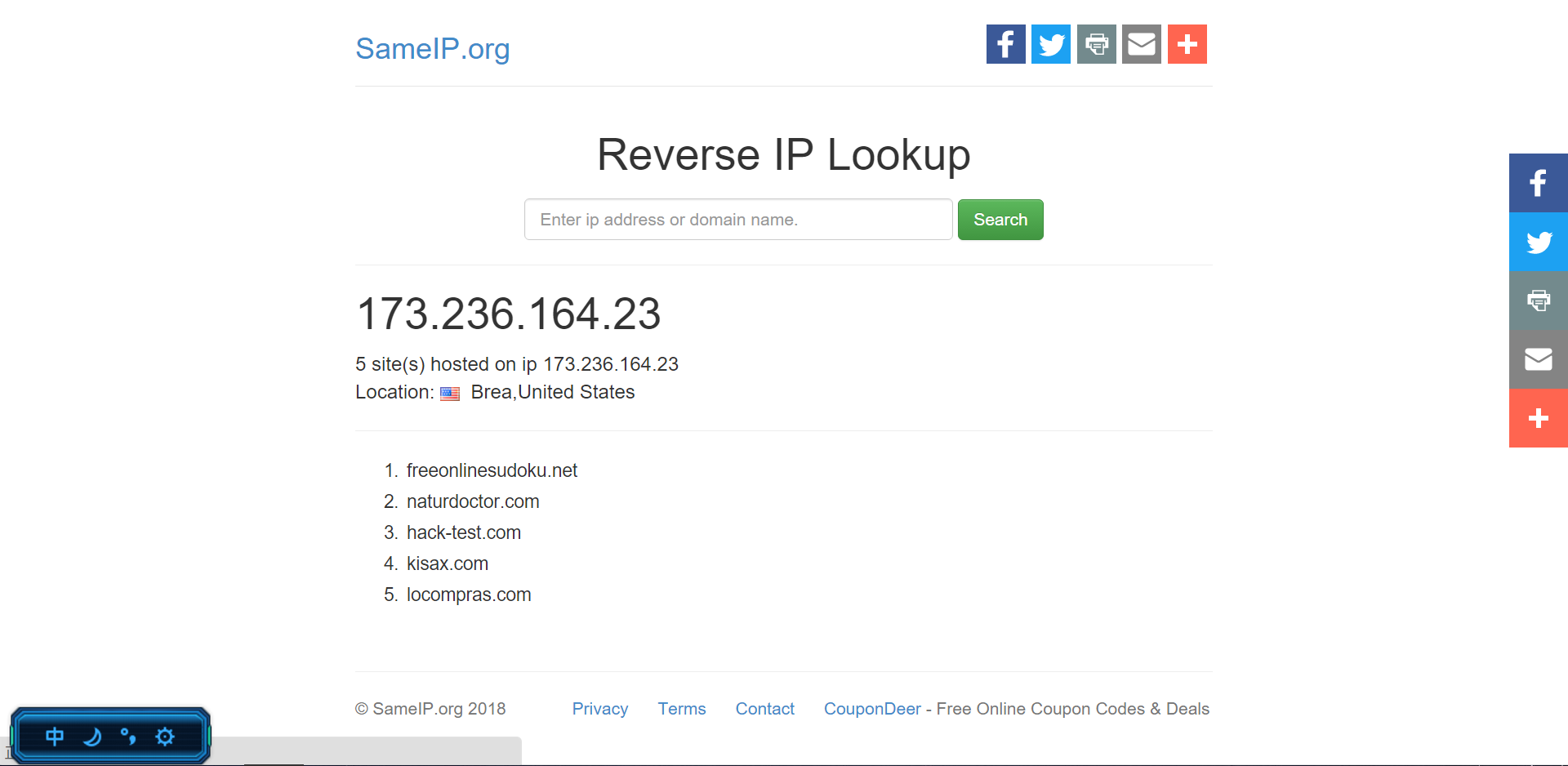
***一、收集信息***

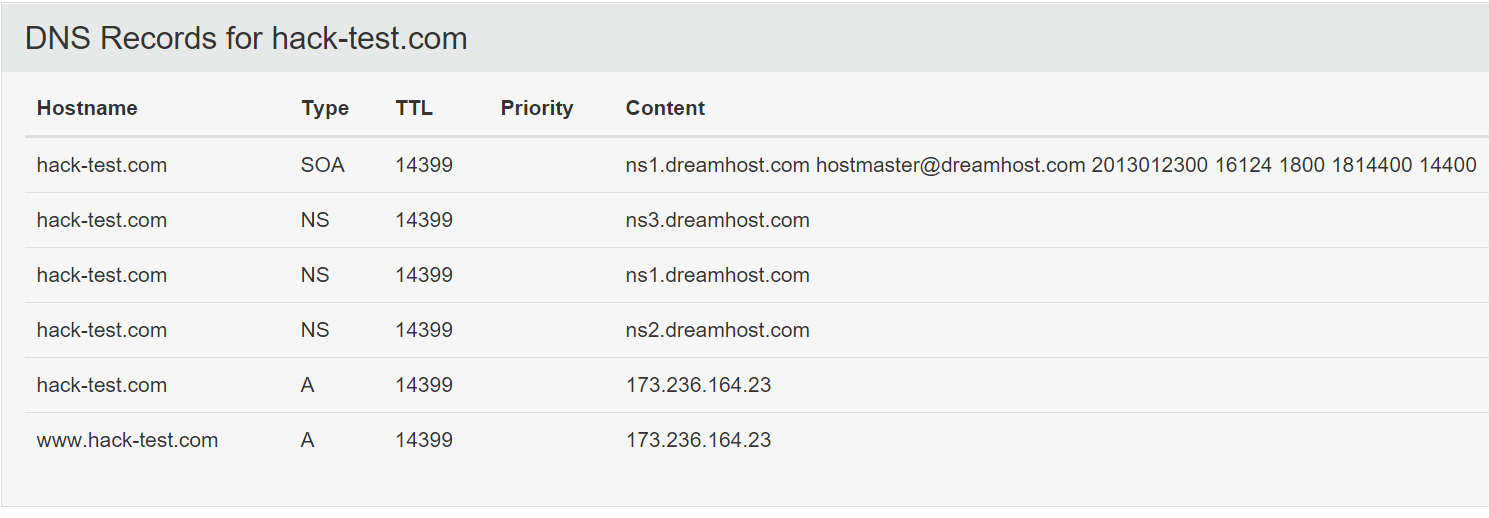
1.ping hack-test.com

得IP为173.236.164.23

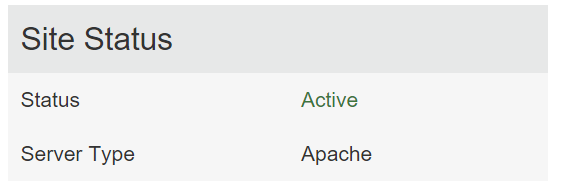
2.通过IP找寻同服务器其他网站（http://www.sameip.org/）



3.查询DNS记录（https://who.is/）



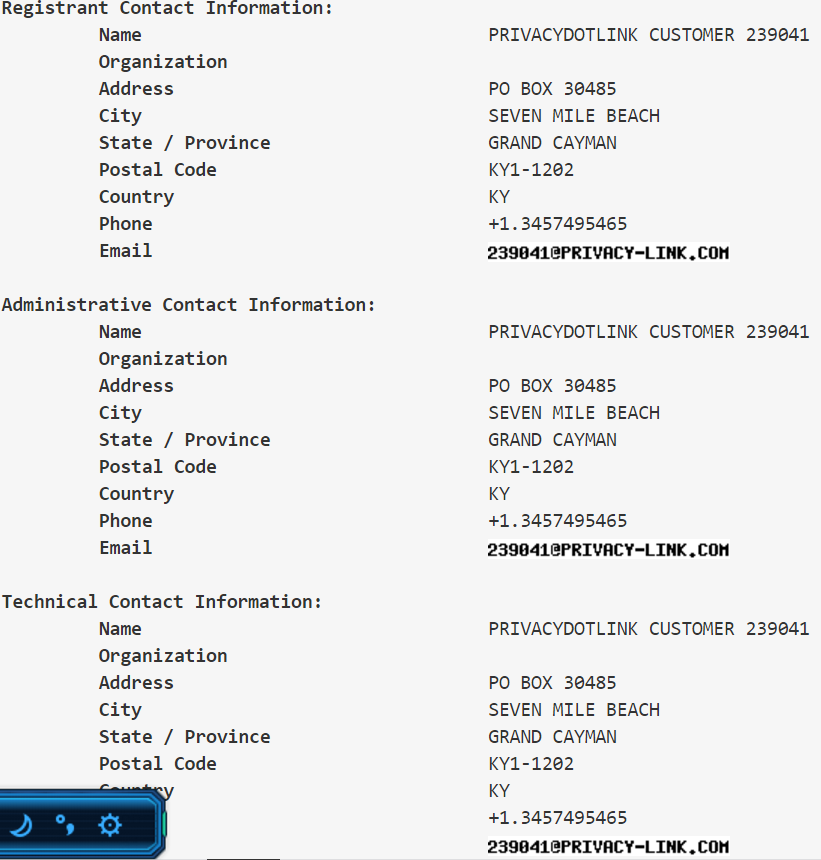
4.查询web服务器类型（https://who.is）



服务器类型Apache

网站现状 active

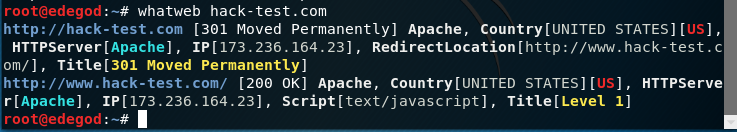
5.网站域名注册信息（https://who.is）



6.使用kali linux 的whatweb获取网站服务器操作系统类型和服务器版本

kali linux

whatweb hack-test.com



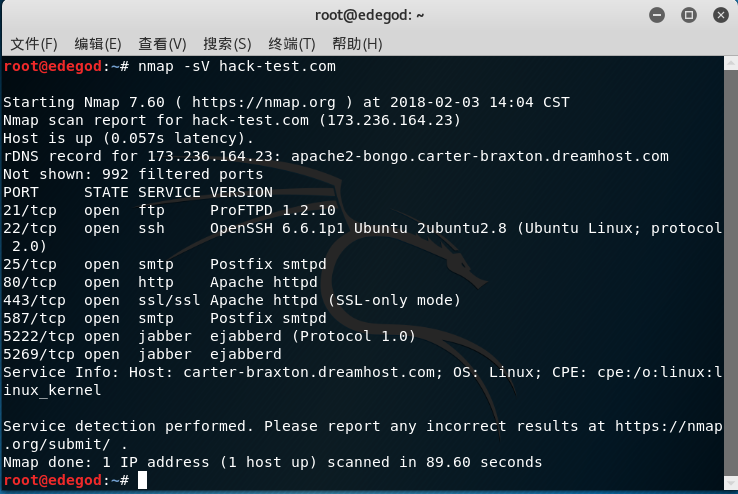
7.了解该网站的建站程序PHP的？（需要对各种CMS程序了解，PS：看他的程序语言就这样看 [www.baidu.com/xx.asp?xx=xx](http://www.baidu.com/xx.asp?xx=xx" \t "https://zhidao.baidu.com/question/_blank) [ASP脚本] [www.baidu.com/?xx.html?=xx](http://www.baidu.com/?xx.html?=xx" \t "https://zhidao.baidu.com/question/_blank) [ASP脚本] [www.baidu.com/xx.php?xx=xx](http://www.baidu.com/xx.php?xx=xx" \t "https://zhidao.baidu.com/question/_blank) [PHP脚本] [www.baidu.com/xx/xx](http://www.baidu.com/xx/xx" \t "https://zhidao.baidu.com/question/_blank) [PHP脚本比较高的几率]判断CMS责得对CMS要了解些，一般的判断方法就是看默认布局风格其次看网页底部版权，能知道后台的话最容易，看一眼就知道了因为上面标着什么CMS系统，还有能重会员系统中判断出来每个CMS都有自身的特征，稍微留一下就知道了）

百度经验链接：https://jingyan.baidu.com/article/e52e36157d01c040c70c5161.html

8.查询服务器上运行的服务

kali linux

nmap -sV hack-net.com



9.查询操作系统版本以及开放的端口（扫描时间长）

kali linux

nmap -O hack-net.com



二、渗透准备

10.扫描寻找漏洞

