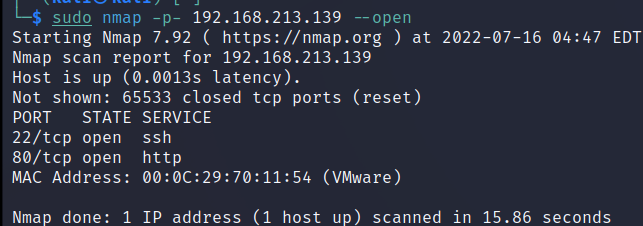
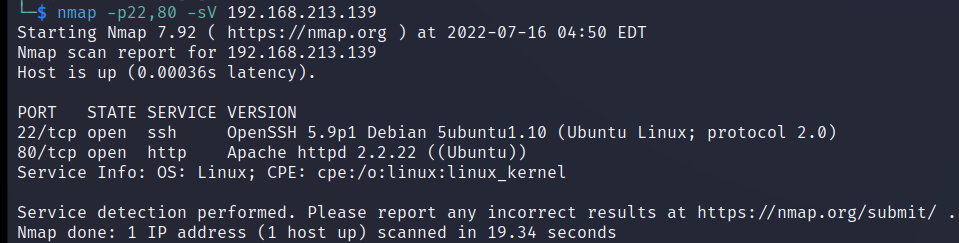
1. sudo nmap -p- 192.168.213.139 --open



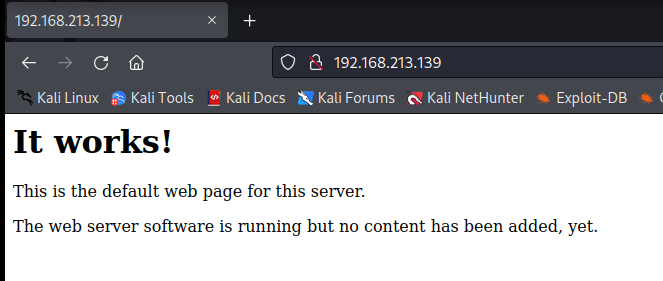
1. nmap -p22,80 -sV 192.168.213.139



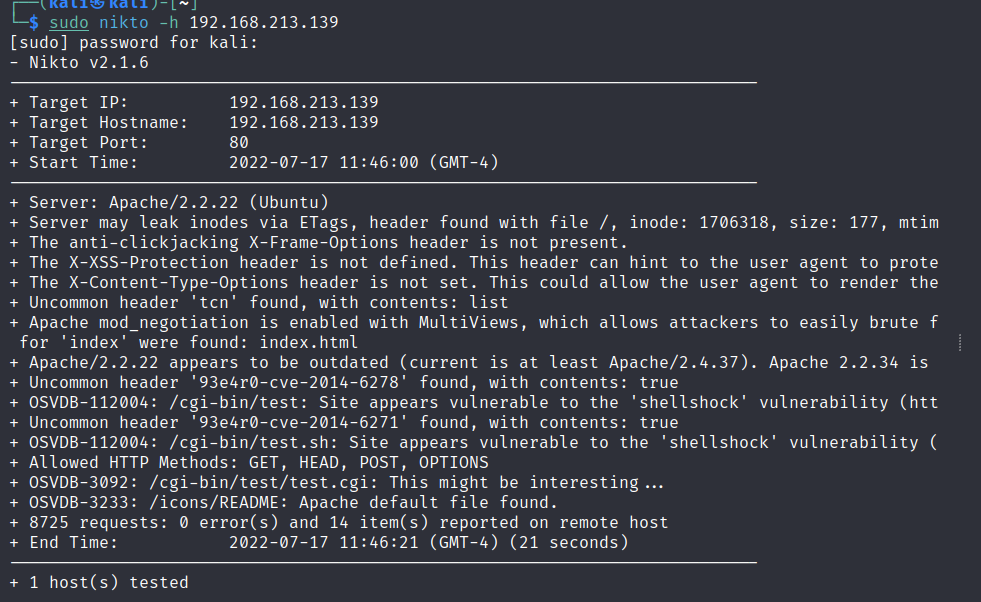
1. 查询openssh相关漏洞



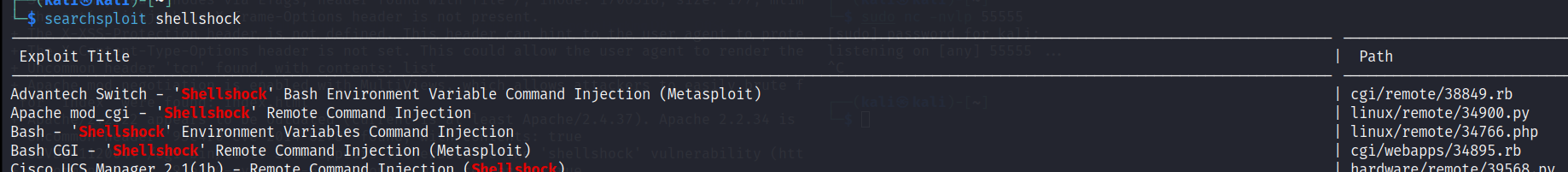
1. 查询apache httpd相关漏洞，未找到可利用点
2. 访问<http://192.168.213.139>,页面无可用信息



1. 使用nikto扫描目标主机，发现可疑文件/cgi-bin/test/test.cgi及可能存在漏洞shellshock



1. searchsploit shellshock搜索漏洞数据库，找到相关漏洞程序linux/remote/34900.py



1. 使用漏洞程度建立反弹shell连接

