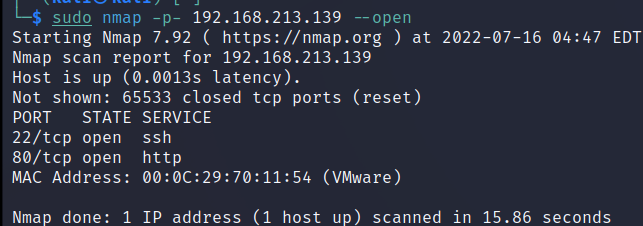
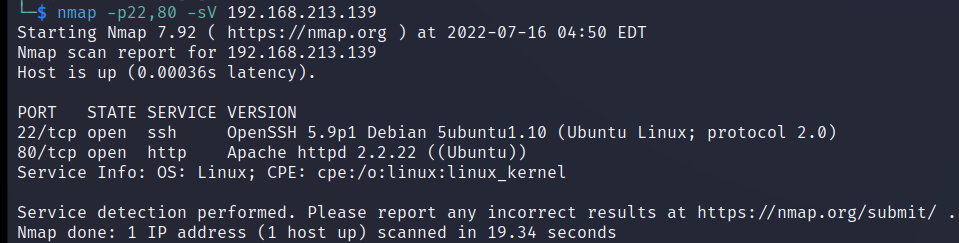
1. sudo nmap -p- 192.168.213.139 --open



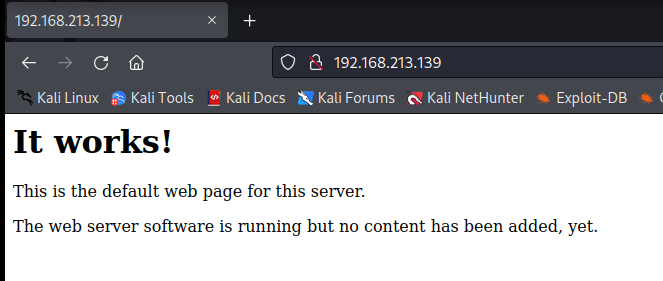
1. nmap -p22,80 -sV 192.168.213.139



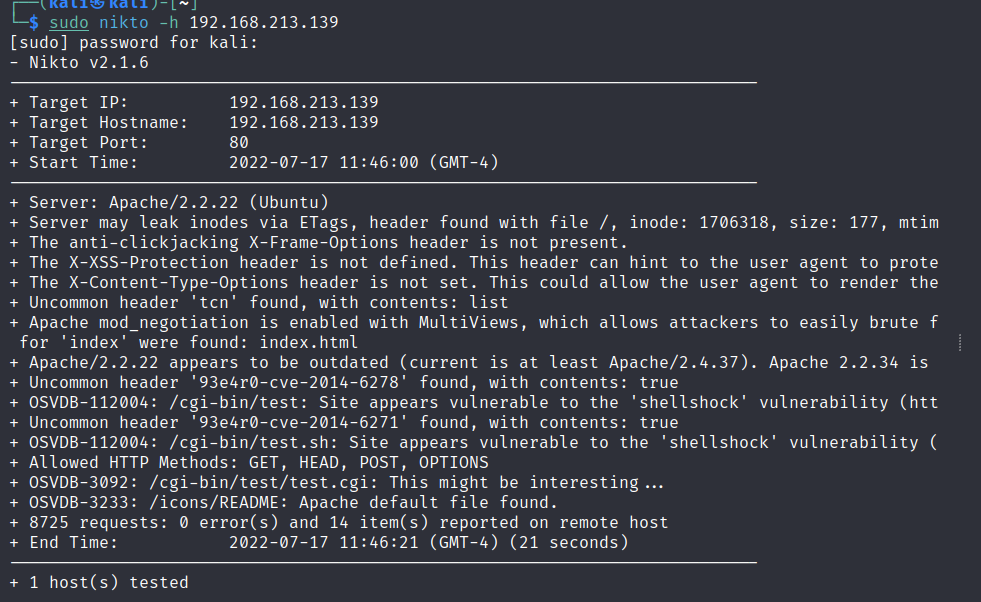
1. 查询openssh相关漏洞,未找到突破边界的漏洞



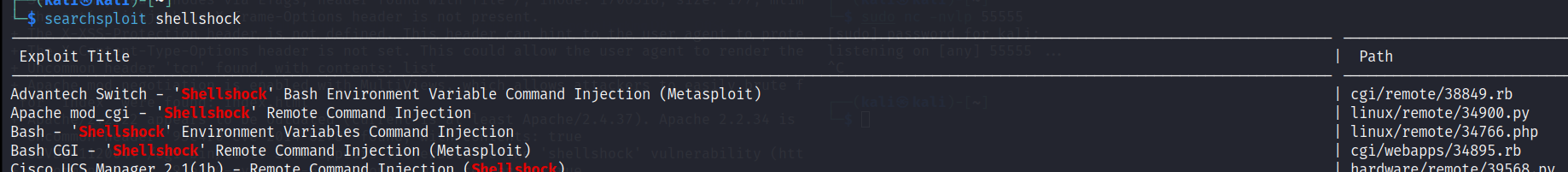
1. 查询apache httpd相关漏洞，未找到可利用点
2. 访问<http://192.168.213.139>,页面无可用信息



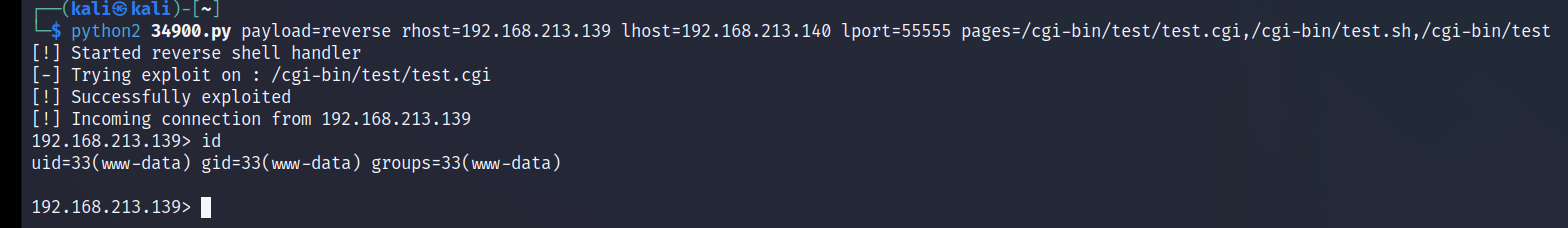
1. 使用nikto扫描目标主机，发现可疑文件/cgi-bin/test/test.cgi及可能存在漏洞shellshock



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

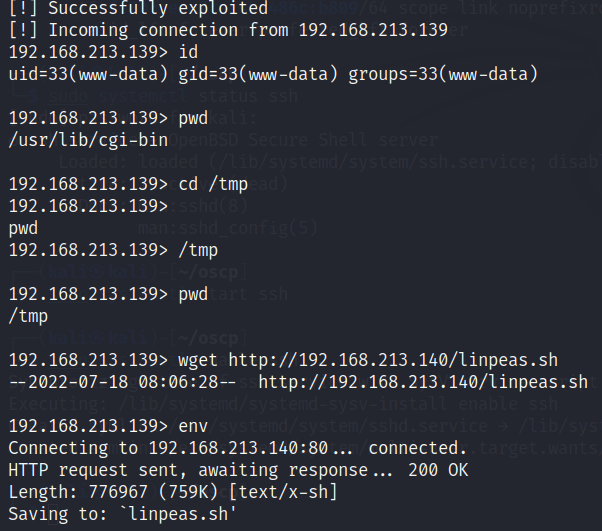


1. 使用漏洞程度建立反弹shell连接

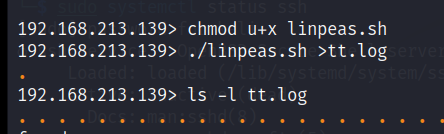


9.下载脚本https://github.com/carlospolop/PEASS-ng/releases/latest/download/linpeas.sh

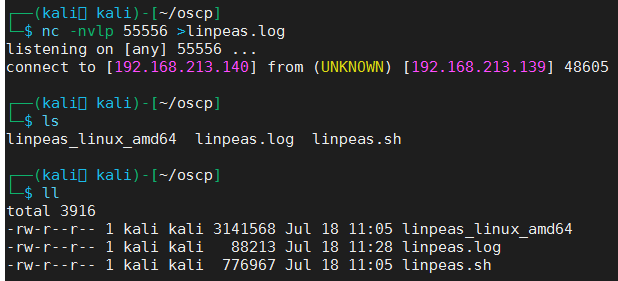
，kali上开启http服务，将脚本放到网页根目录，在目标机上使用wget下载脚本文件



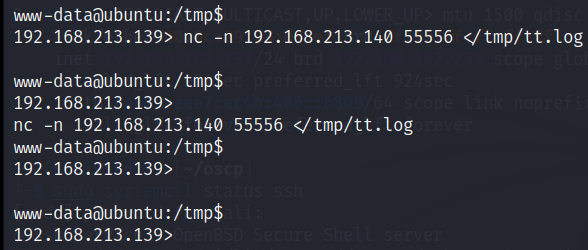
10.给脚本增加执行权限，执行并将结果重定向至tt.log文件



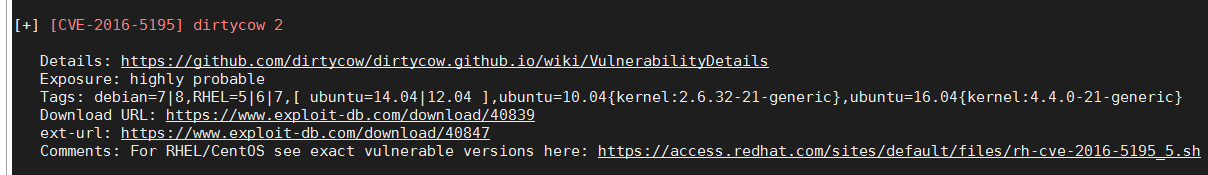
11，kali上使用nc监听端口55556，并将输出重定向至文件



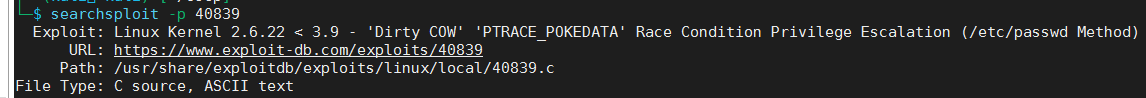
12.目标机上使用nc将日志文件传输至kali



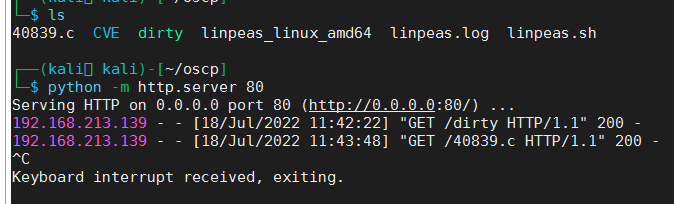
13.查看日志文件tt.log并找到可利用漏洞及漏洞编号



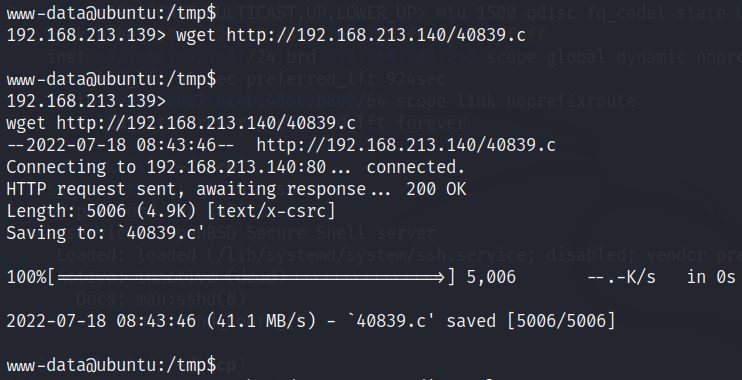
14.在kali本地漏洞数据库中查找到对应漏洞利用文件



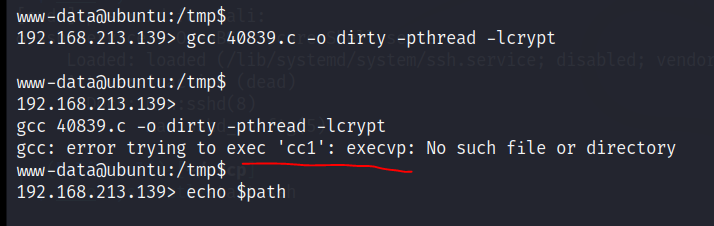
15.kali上开启http服务并将漏洞利用文件放至网页根目录



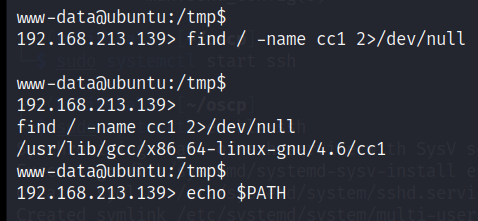
16.在目标机上使用wget下载漏洞利用文件



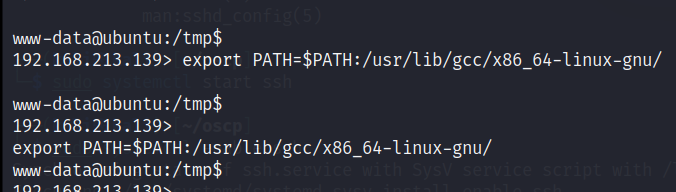
17.编译漏洞利用文件，出现如下错误信息



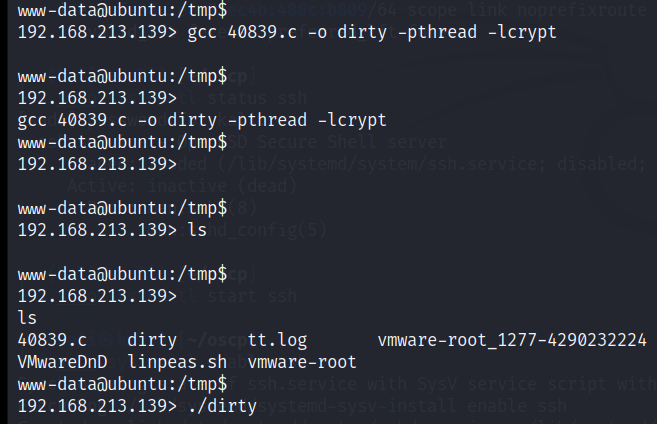
18.在目标机上查找cc1,得到其所在目录



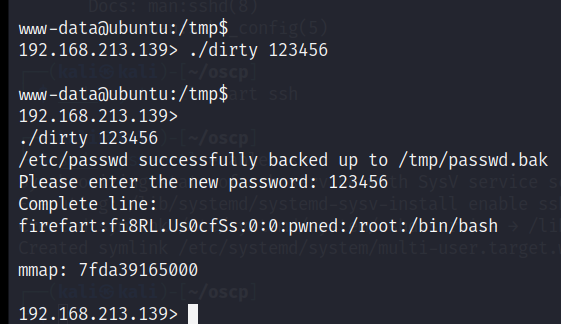
19.使用export将cc1所在目录加入到PATH环境变量中



20.再将编译漏洞利用文件



21．在目标机上执行漏洞利用程序，程序添加具有root权限的账号firefart



22.使用新添加的账号firefart登陆目标机，取得root权限

