SCENARIO #3: **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

☐Advance

Time Required: 60 minutes

Audience: ☒Instructor-led ☐Self-taught

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

Demonstrate the hacking of PBX admin system (in fact, any password-protected systems) with the help of Browser and Hydra.

Materials List:

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

Systems and Tools Used:

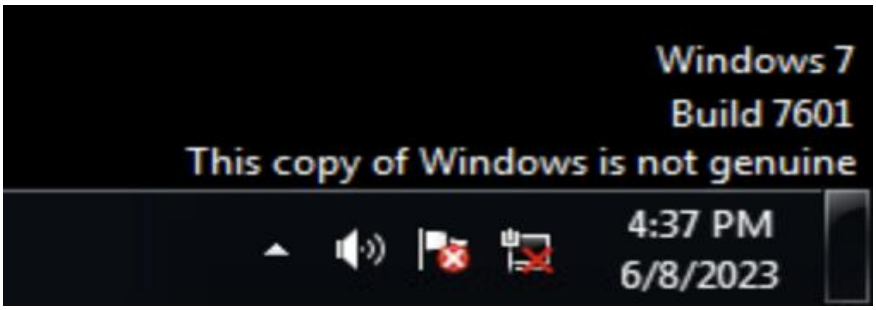
- Kali Linux (CleKali936; u: root, p: toor)
  - Hydra
- Windows 9 (CleWindows929; u:administrator, p: Pa$$w0rd)
- PBX System (ClePBX523; u:root, p:root@123)
- Power down all other systems

Environment Setup:

Please refer to the OCRI Sandbox Setup document. In this lab, we will be using Kali Linux, PBX and Windows 9 machine instances.

Environment Setup Verification: Before starting this pen test make sure the environment setup is done and deployment is successful.

- Verify that the remote connection to Kali Linux machine is successful and the machine is connected to internet without any error. If there is an error in the Internet Connection that means the deployment is not proper.
- Verify that the remote connection to windows machine is successful and the machine is connected to internet without any error. The image below shows an error with internet connectivity.



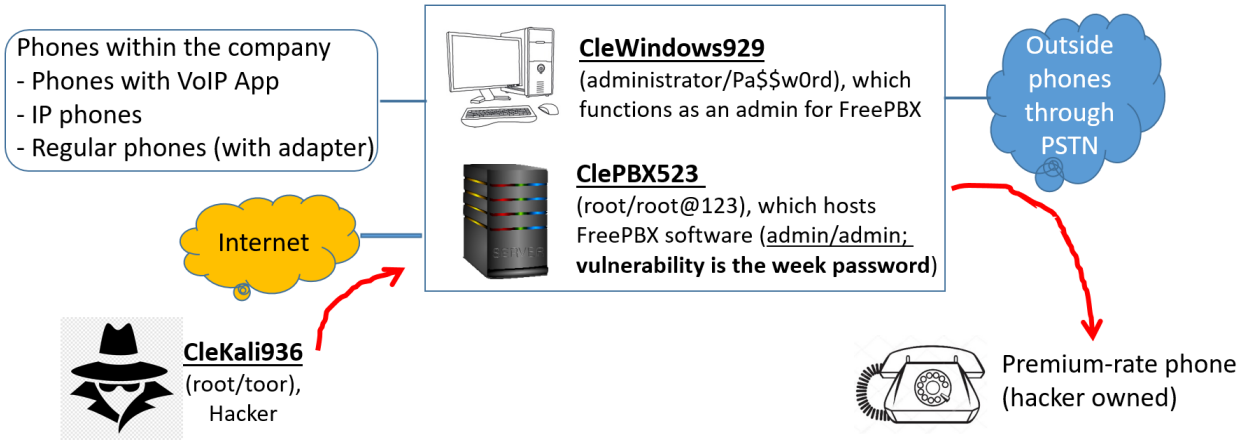
- Do not start the pen test if deployment is not successful. Delete the deployment and redeploy it again.

Introduction:

This laboratory experiment delves into the security vulnerabilities associated with a Private Branch Exchange (PBX) administrative system. While potential threats such as firewall bypass and vulnerabilities in FreePBX, such as XSS, exist, the primary focus of this lab is on a prevalent and straightforward vulnerability: weak passwords.

The central characters in this experiment are three key machines: ClePBX523, CleWindows929, and CleKali936, as illustrated in the figure below. ClePBX523 serves as the pivotal host for FreePBX, delivering PBX services to an organization. Its critical role lies in functioning as the nerve center for telecommunications within a small firm, overseeing call routing, voicemail, and other essential operations. Additionally, the interconnected CleWindows929 system is responsible for configuring the PBX system for users within the firm.

The security of this PBX system comes into question as CleKali936 enters the scenario. Leveraging the browser's network tool, it intercepts HTTP requests, allowing it to scrutinize the traffic between the administrator's browser (CleWindows929) and the PBX system (ClePBX523). The hacker operating from the CleKali936 machine employs Hydra, a potent password-cracking tool, to identify the password and make unauthorized attempts to access the admin panel. The unfolding scenario is divided into four parts, each of which will be thoroughly introduced in the following sections.



Steps to perform the hacking of PBX Admin Systems in the Sandbox:

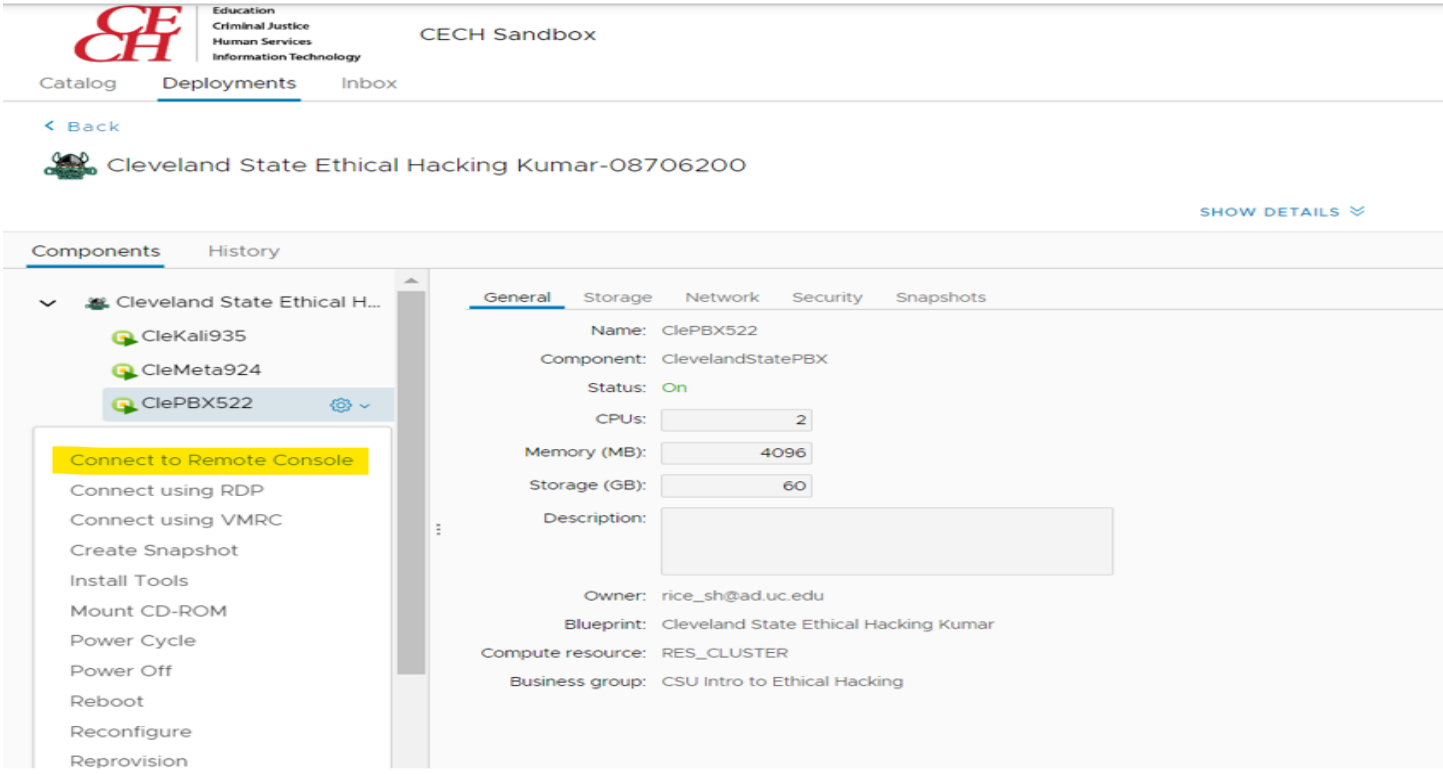
In this scenario, we will walk through a systematic four-part process, each of which contributes to a comprehensive security analysis of a PBX system. **Part One** involves setting up the PBX environment on the host machine, ClePBX523, and the admin machine, CleWindows929. **Part Two** guides us through configuring the system using Mozilla Firefox on the hacker machine, CleKali936. **Part Three** uses the browser-based tool, Inspect Element, to monitor the network traffic from the PBX host. Lastly, **Part Four** involves employing a password-cracking tool, Hydra, to attempt unauthorized access to the PBX system's admin panel.

At the end of each step, tasks are present. Please complete the tasks.

> Warning: The numerical component linked to the machine name (e.g., 523 in ClePBX523) may vary from the actual access details when navigating the Sandbox in the OCRI platform.

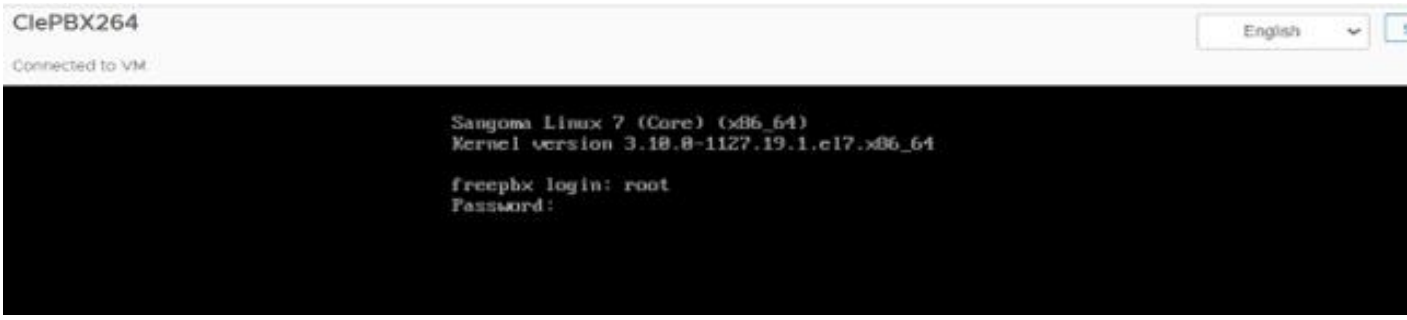
Part One: Setup PBX (ClePBX523 & CleWindows929)

1. Login into the Sandbox using the OCRI credentials and connect to “ClePBX523” using “Connect to Remote Console” as shown below.

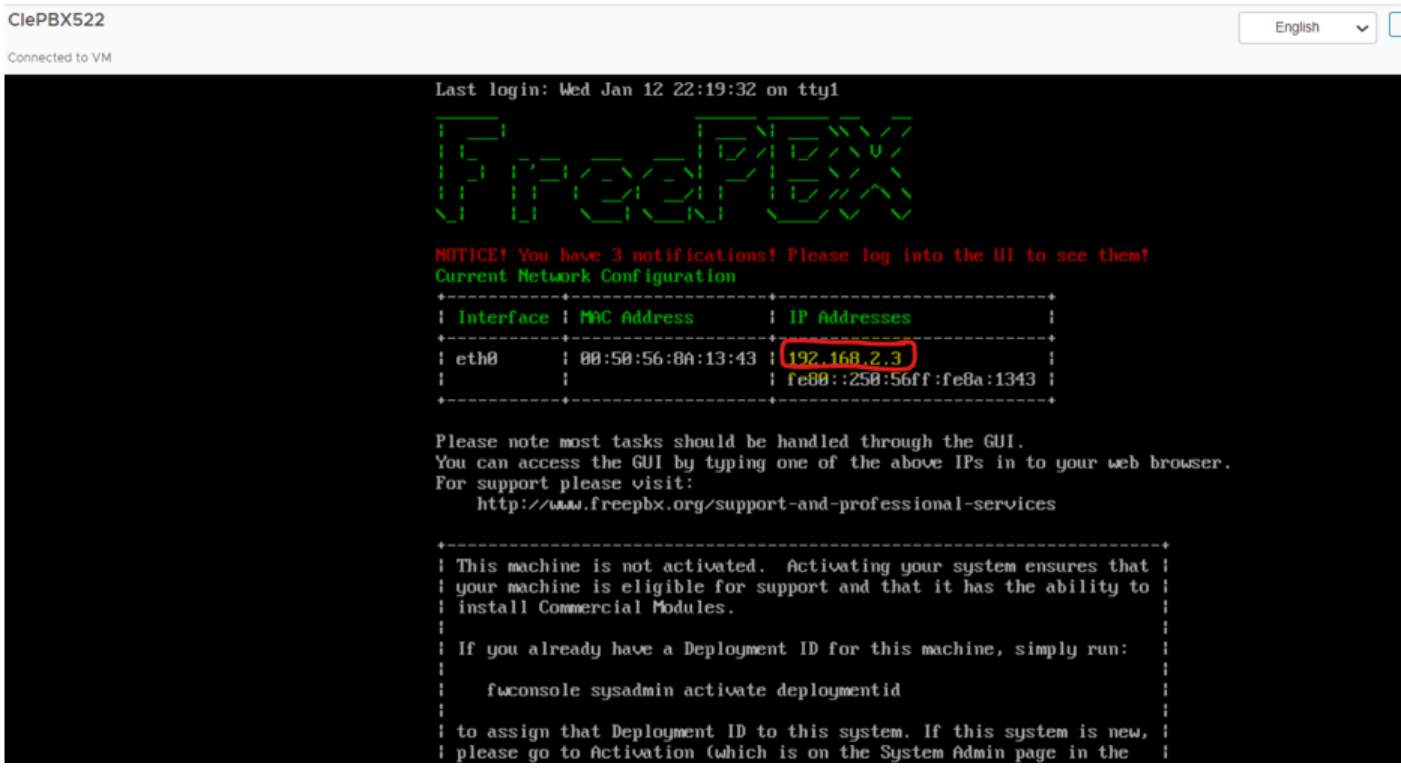


2. Login to “ClePBX523” using the credentials below.

Username: root
Password: root@123

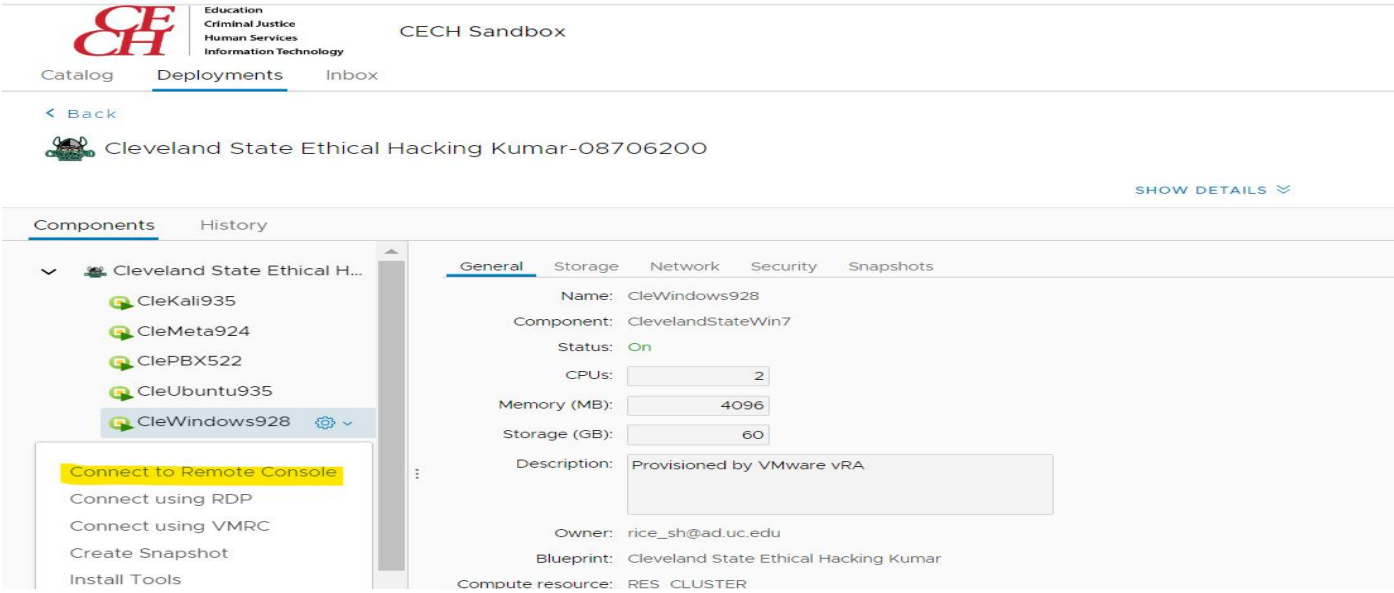


3. Once login is completed, below screen appears. Note down the IP address of the system for future use.

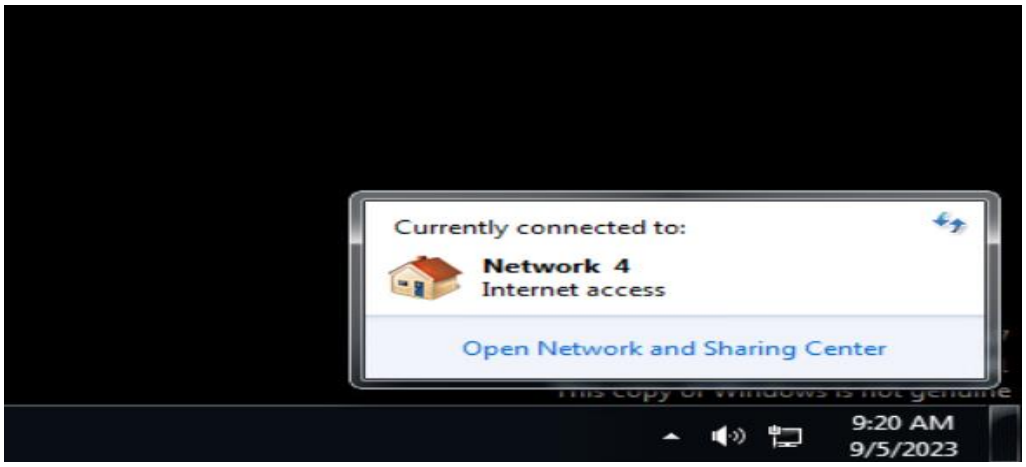


4. Go to Sandbox and connect to “CleWindows929” machine using “Connect to Remote Console” as shown below. Use the below credentials to login to “CleWindows929”.

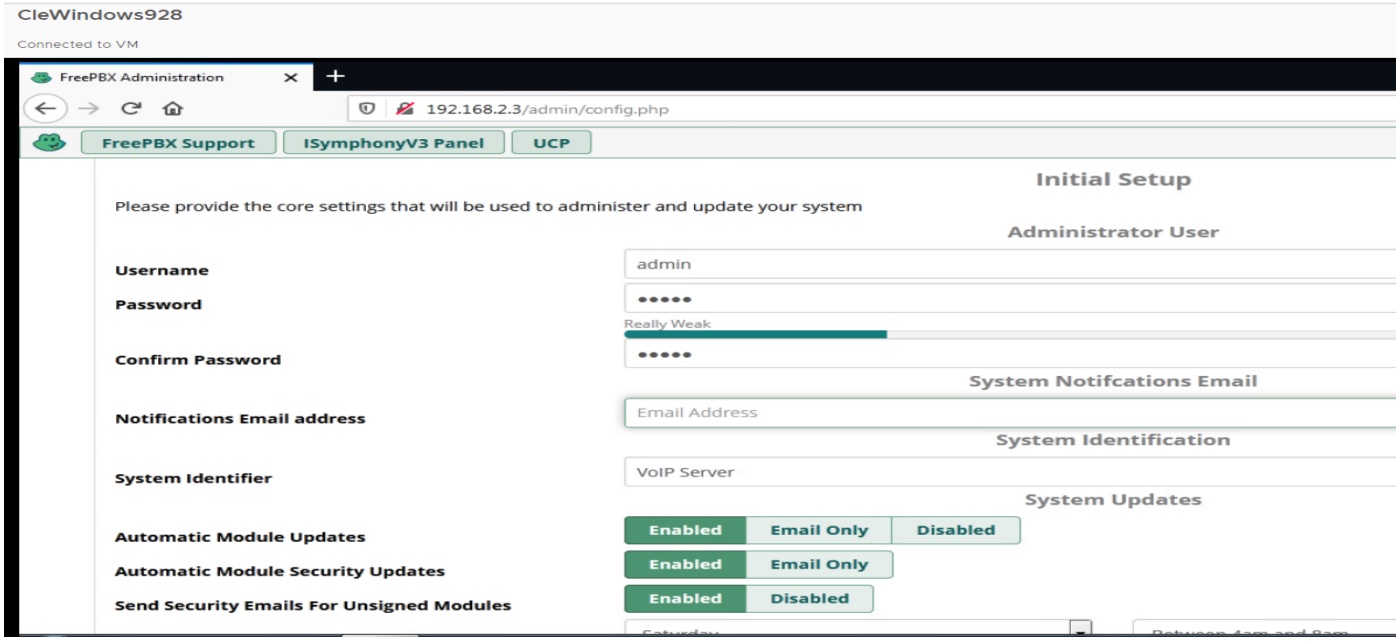
Username: administrator
Password: Pas$$w0rd



5. Verify that the logged in windows machine has internet access. It should say “Currently connected to: Internet access” as shown below.



6. Launch the Firefox browser and input the IP address into the URL field, which is taken in step 3 as depicted below.

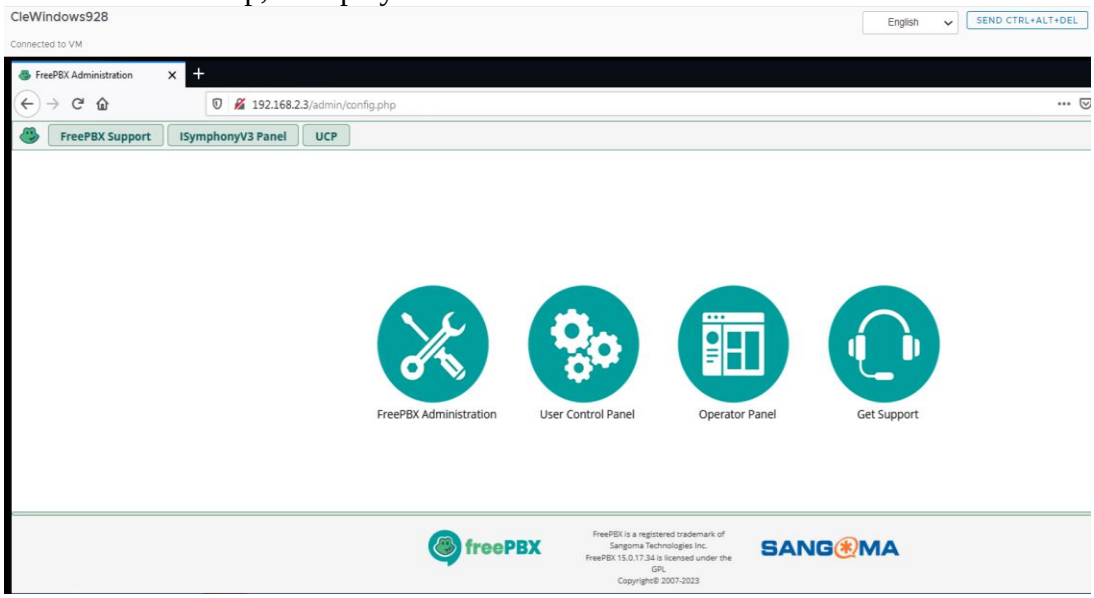


7. Setup a username and password for the PBX system. Fill in the details – username, password, confirm password, notification Email address and click on “Setup System”.

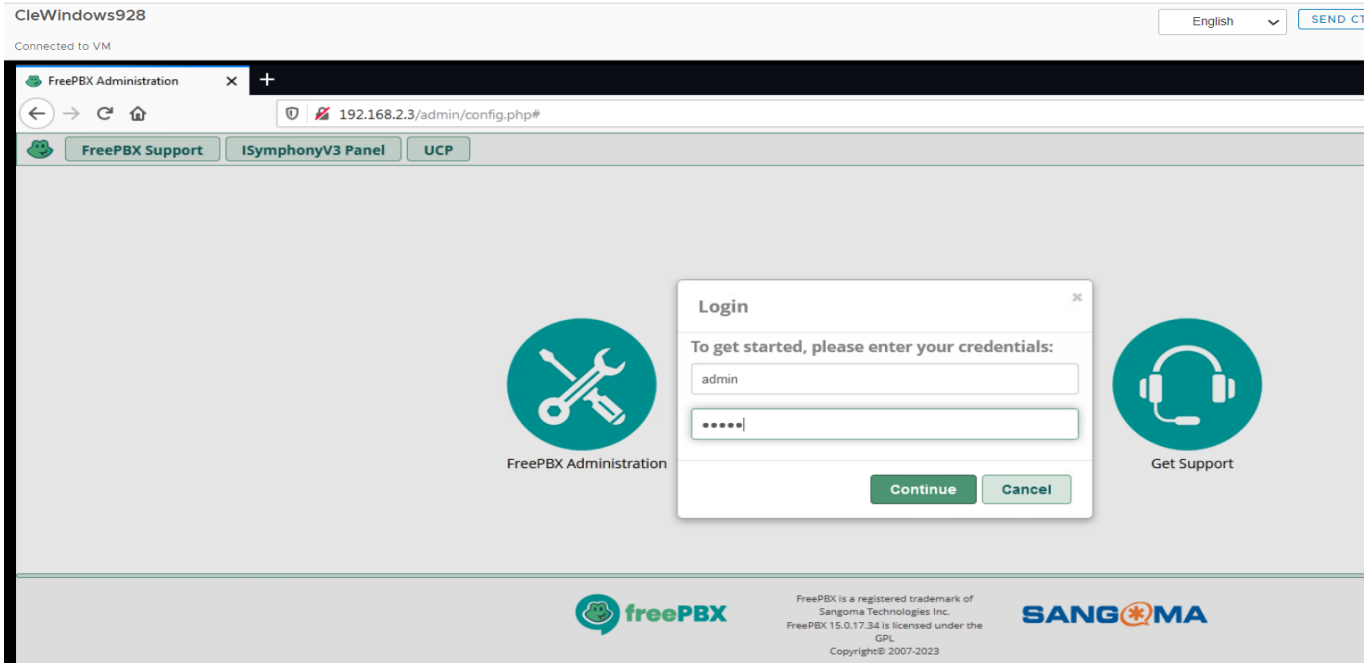
Username: admin
Password: admin

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

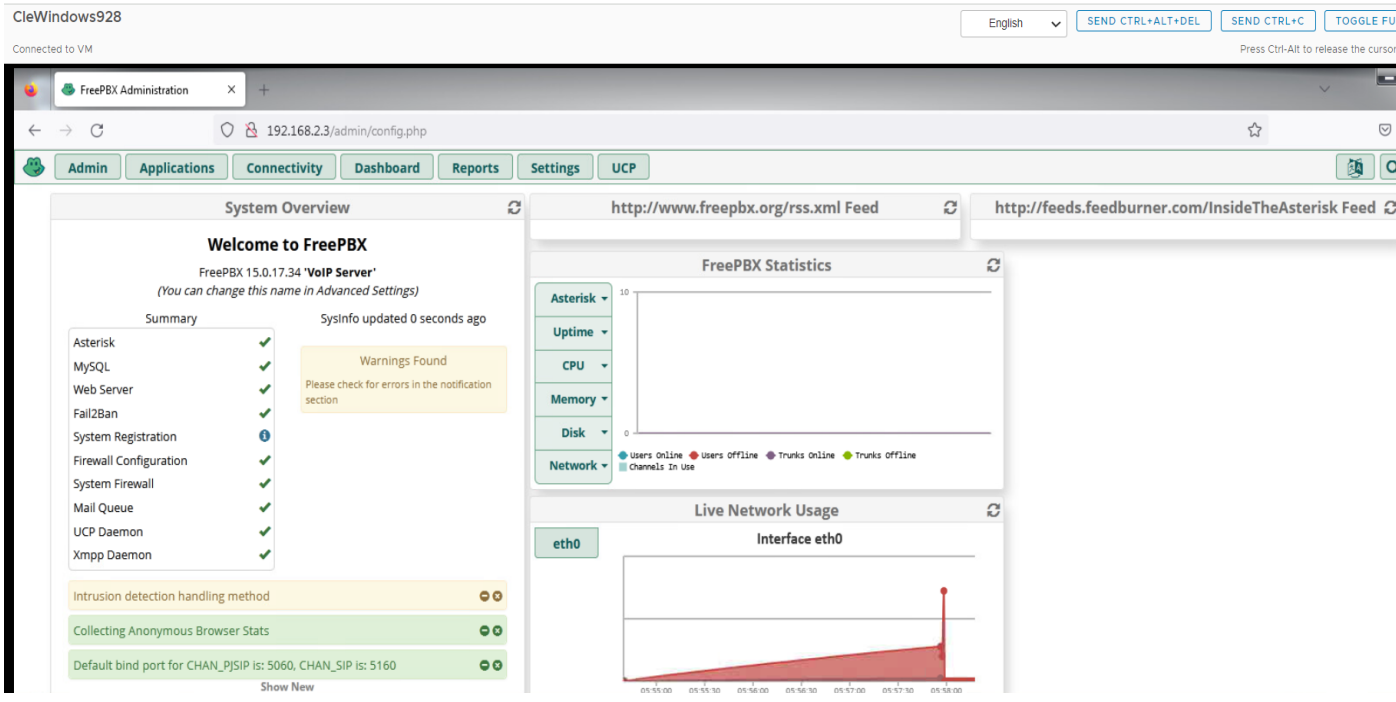
8. After the initial setup, it displays the “Free PBX Administration” Panel as shown below.



9. Click on the “FreePBX Administration” and login via username: admin and password: admin which are set in step 7 and click on “Continue”.



10. Complete the setup by clicking submit, continue, YES or next. (Click any of the following buttons until you come up with the following screen). Below is the “System Overview” screen, once the below screen appears, the setup is done.



Tasks:

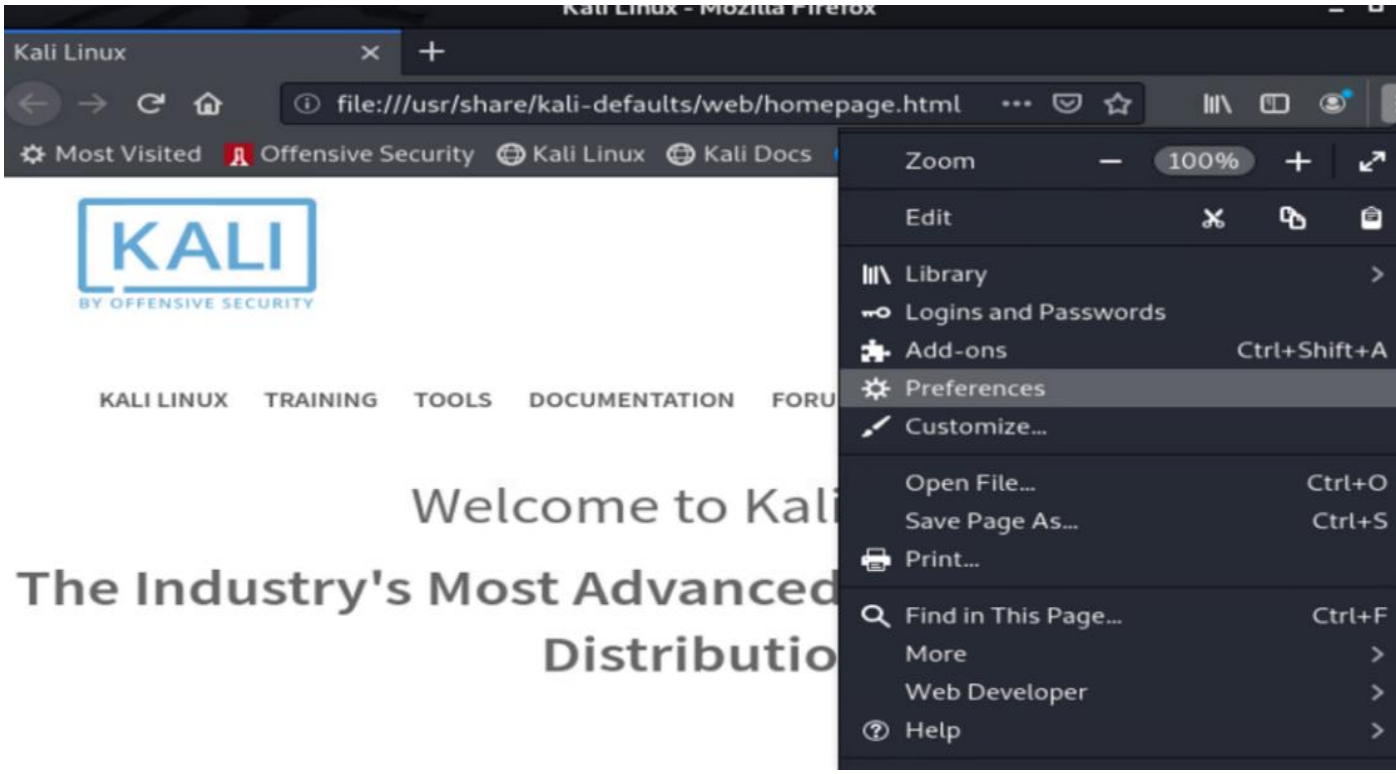
1. Please provide the screen shot of the “System Overview” screen achieved in step10.

Part Two: Configuring System for Web Application Analysis (CleKali936)

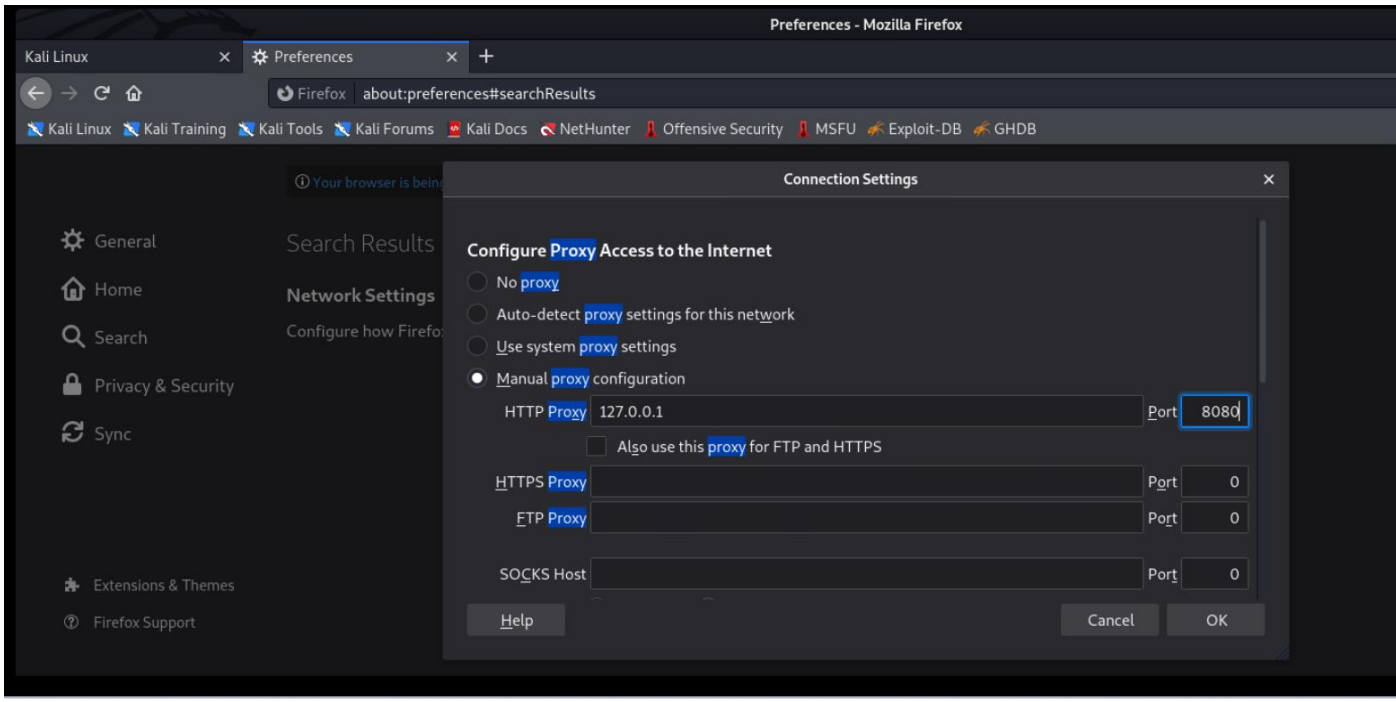
11. Go to Sandbox and connect to “CleKali936” using “Connect to Remote Console”. Use the credentials below to login to “CleKali936” (Kali Linux system).

    Username: root, Password: toor

12. Launch the Mozilla Firefox window, and in the upper right corner, open the "Open Menu." Inside the menu, find "Preferences," and proceed to select it.



13. Perform a search for "Proxy," and subsequently, select "Settings." Opt for the manual proxy configuration. Input the IP address 127.0.0.1 for the HTTP Proxy and set the port to 8080. Conclude by clicking "OK" and close the browser window.



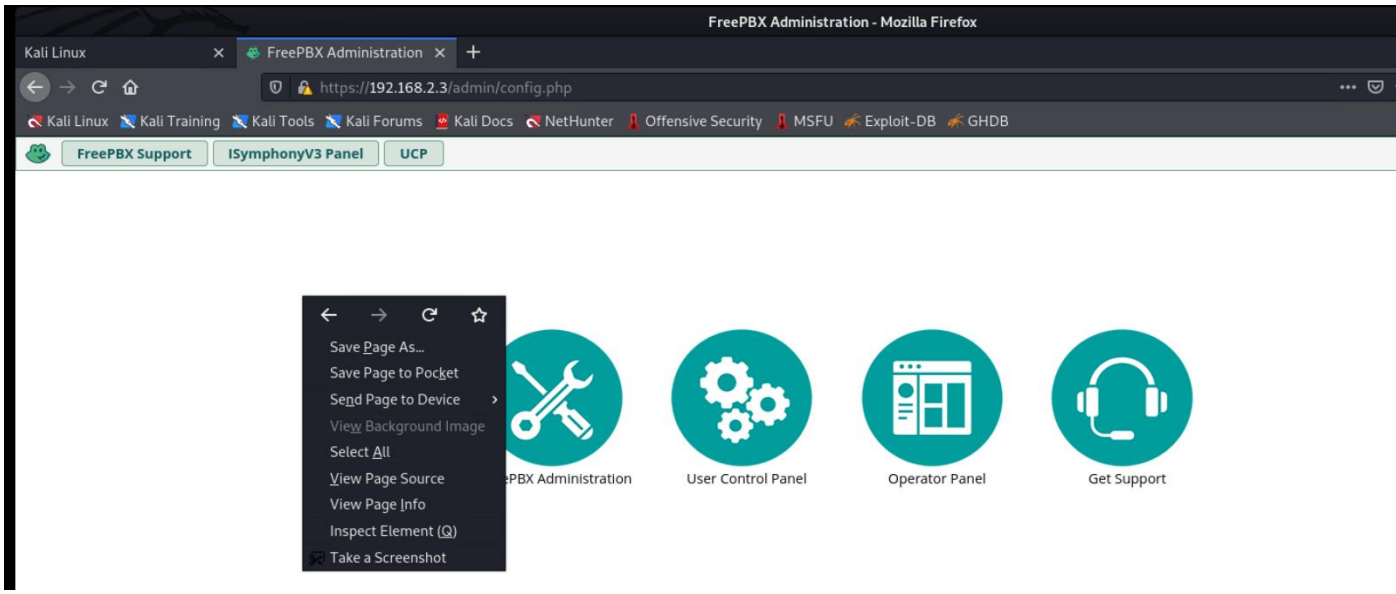
Note that 127.0.0.1 is a special IP address that indicates the local computer, in this case CleKai936. By setting yourself as the proxy, you intend that all your communication pass through yourself before reaching the destination computer, allowing you to check the traffic. Port 8080 is the standard HTTP port.

Tasks:

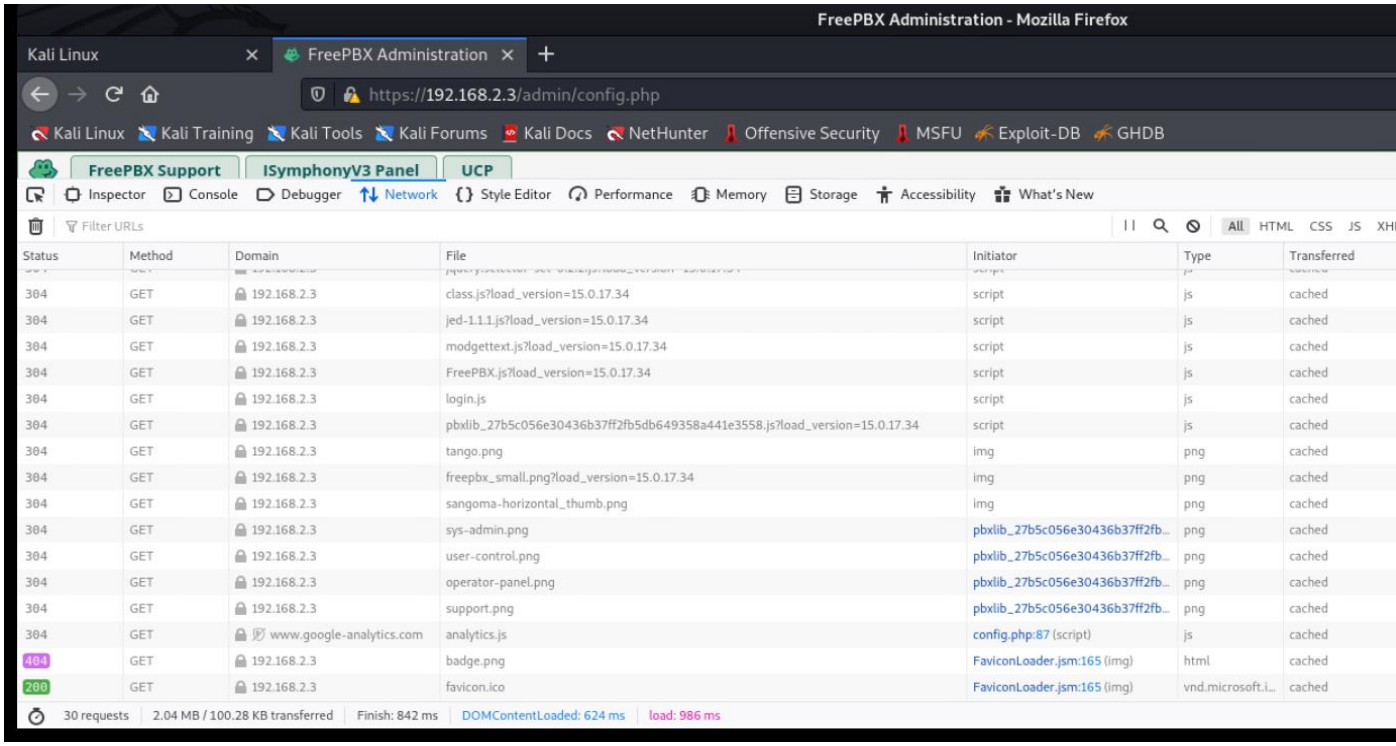
2. Please provide the screenshot of proxy settings done at the step 13.

Part Three: Analysis using Inspect Element (CleKali936)

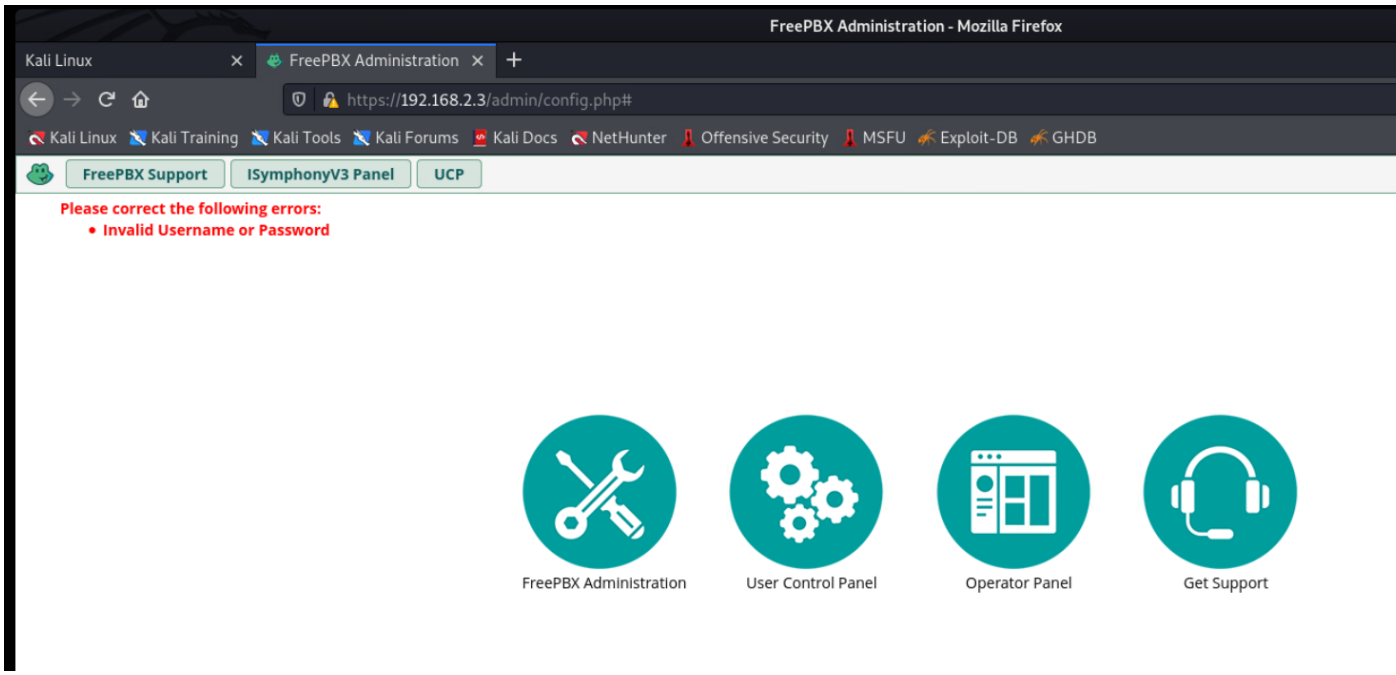
14. Launch the Firefox browser and input the IP address into the URL field, which is taken in step 3, it opens the “FreePBX Administration” and then right click on “Inspect” or “Inspect Element” as shown below.



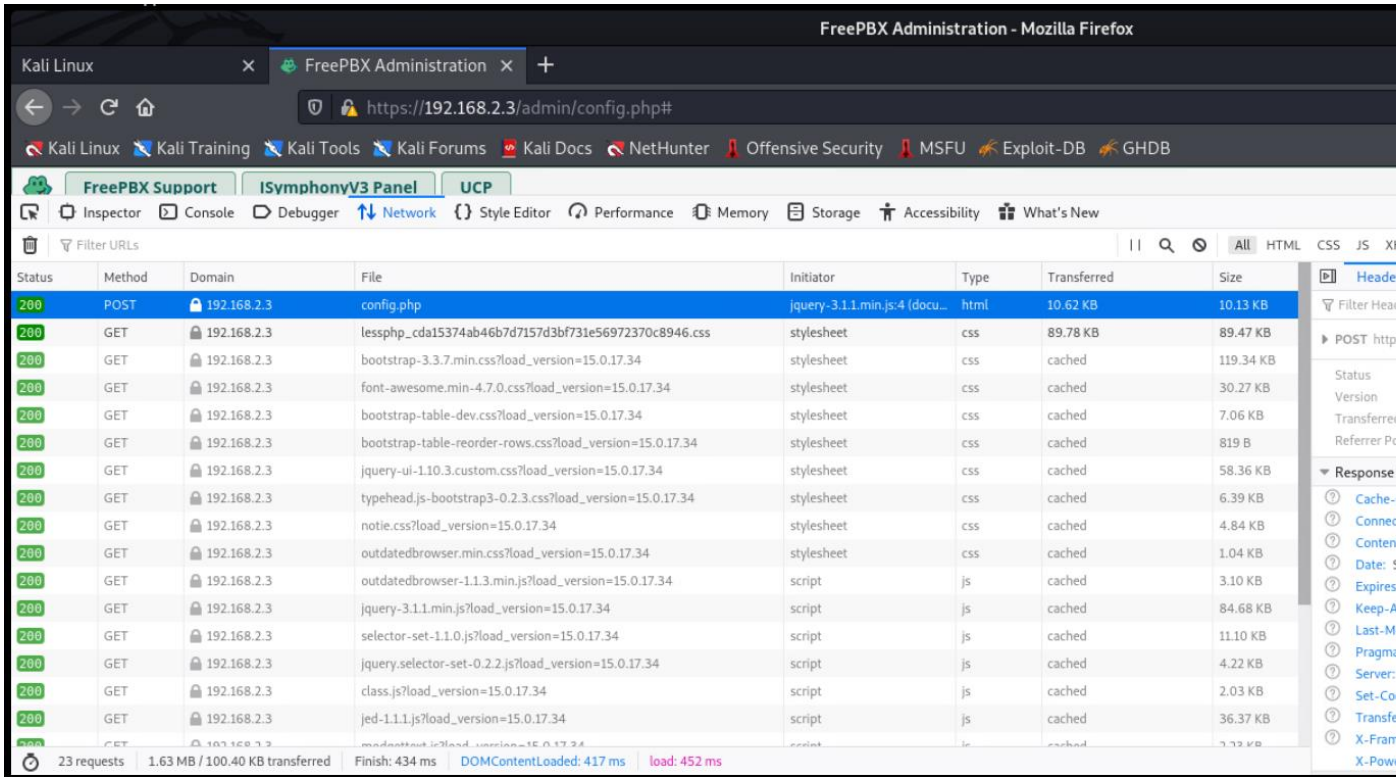
15. Click on “Network” tab on subpanel at the bottom and then click on Reload. Owing to step 13, all the network traffic (HTTP) are monitored.



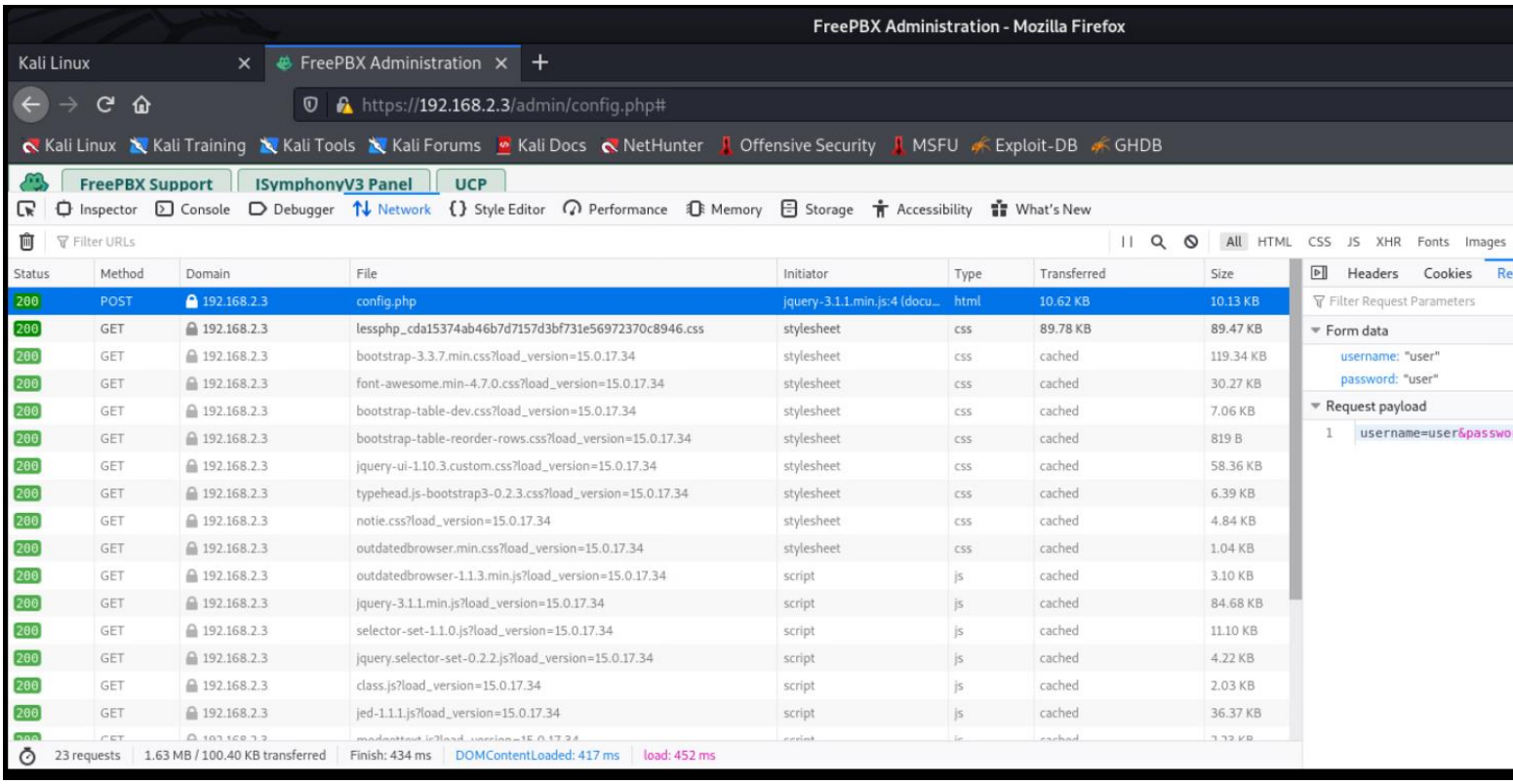
16. Click on “Free PBX Administration” panel and try to login with any credentials, it throws an error message as shown below. Here, credentials used are username:user and password:user.



17. Go to the Network tab at the bottom (as in step 15) and look for a Post request, and you'll discover a Post request directed at config.php as highlighted in the below.



18. Click on Request tab on the right hand side to investigate the phony credentials being sent to elements in config.php. We can see fake credentials (u:user, p:user) being passed to Request.



Tasks:

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

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

Part Four: Hacking with Hydra (CleKali936)

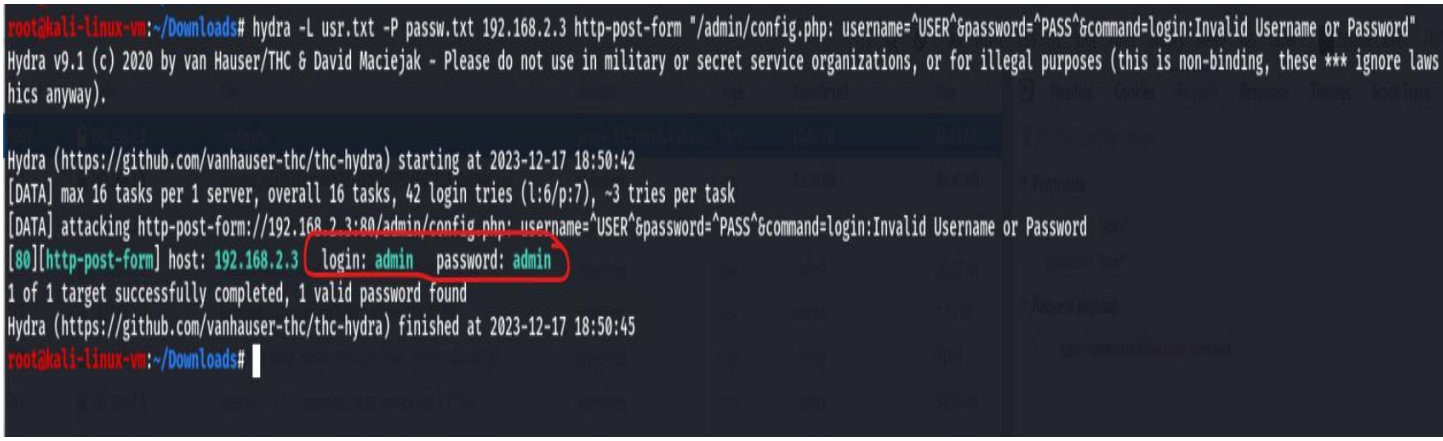
We are going to utilize Hydra to try several trivial username and password combinations, assuming the PBX admin inadvertently picked a simple username and password. Given a pair of text documents, with one designated for usernames and the other intended for passwords, Hydra will generate all possible combinations and attempt to access the PBX admin system.

19. Create a pair of text documents and name them as usr.txt and passw.txt, respectively. The following is the sample use.txt and passw.txt.

20. Open the terminal window, navigate to the file location where use.txt and passw.txt are present using the "cd" command (change directory).

21. Execute Hydra as shown below. The output, as depicted in the screenshot below, reveals a successful attempt. It shows all unsuccessful attempts too.
In this command, -L specifies the file for usernames and -P specifies the file for passwords. 192.168.2.3 is the IP address of the PBX host (ClePBX523), which was obtained in step 3.

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"



Tasks:
5. Please provide the screenshot of the login credentials which are obtained using Hydra.

Glossary:

- **Kali Linux:** Kali Linux is a specialized Linux distribution designed for advanced penetration testing, ethical hacking, and network security assessments. It was developed and is maintained by Offensive Security, a leading provider of information security training and certification. We can find more information about Kali Linux on their official website. https://www.kali.org/docs/introduction/what-is-kali-linux/

- **PBX:** PBX stands for Private Branch Exchange, which is a telecommunications system used by organizations to manage and route phone calls internally within their own network. PBX systems have been a staple in business communications for many years, although modern technology has evolved them into more advanced forms, such as IP PBX or VoIP PBX.Here are the key components and functions of a traditional PBX system:
  Call Routing: PBX systems route incoming calls to the appropriate extensions or departments within an organization. This allows for efficient call distribution and reduces the need for multiple phone lines.
  Extension Dialing: Users within the organization can dial each other's extensions directly without going through the public phone network. This simplifies internal communication.
  Voicemail: PBX systems often include voicemail services, enabling users to leave messages when the recipient is unavailable. Users can then retrieve their voicemail messages from their own extensions.
  Call Forwarding: Users can forward their calls to another extension or an external number, ensuring that they never miss important calls.
  Conference Calls: Many PBX systems support conference calling, allowing multiple parties to join a single call.
  Interactive Voice Response (IVR): PBX systems may use IVR technology to guide callers through a menu system and direct them to the appropriate department or information.
  Call Recording: Some PBX systems offer call recording capabilities for quality assurance, training, or compliance purposes.
  Reporting and Analytics: Modern PBX systems often provide reporting and analytics features, helping organizations track call volumes, call durations, and other relevant data.
  Integration with Other Systems: PBX systems can integrate with other business applications, such as customer relationship management (CRM) software, to enhance productivity and customer service. It's worth noting that while traditional PBX systems relied on physical hardware and wiring, many businesses are now transitioning to IP PBX or VoIP PBX solutions. These systems use the Internet Protocol (IP) to transmit voice data over data networks, offering more flexibility and cost savings compared to traditional PBX systems.

- **Hydra:** Hydra is a popular and powerful password-cracking tool that is included in Kali Linux, a Linux distribution specifically designed for penetration testing, ethical hacking, and cybersecurity tasks. Hydra is used for attempting to gain unauthorized access to various services and applications by trying different username and password combinations. It's often employed by security professionals and ethical hackers to test the

security of systems and to identify weak or easily guessable passwords. Key features of Hydra include:

Support for Multiple Protocols: Hydra supports a wide range of network protocols and services, including SSH, FTP, Telnet, HTTP, RDP, SMB, and more. This flexibility makes it a versatile tool for testing the security of various network services.

Brute Force and Dictionary Attacks: Hydra can perform both brute force attacks (trying all possible combinations) and dictionary attacks (using a list of pre-defined passwords) to guess login credentials. Dictionary attacks are typically more efficient because they focus on likely passwords.

Parallel and Distributed Attack: Hydra can perform parallel attacks, attempting multiple logins attempts simultaneously to speed up the process. It can also be configured to distribute the attack across multiple machines, making it even more powerful.

Customizable: Users can customize the attack parameters, including the username and password lists, the number of threads, and various attack options, to suit their specific testing requirements.

Logging and Reporting: Hydra provides detailed logging of login attempts and results, making it easier to analyze the outcome of the attack and identify successful login credentials.

It's important to note that while Hydra can be a valuable tool for security professionals when used ethically and responsibly, using it to gain unauthorized access to systems or services without permission is illegal and unethical. It should only be used in environments where you have explicit authorization to conduct penetration testing or security assessments. Additionally, security professionals and ethical hackers should always follow ethical guidelines and legal regulations when performing security testing and respect the privacy and integrity of systems and data they are testing. Unauthorized or malicious use of password-cracking tools like Hydra can have legal consequences.

- **Command Explanation:**

  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: This is the command to execute Hydra.

  -L usr.txt: Specifies the path to a file containing a list of usernames. In this case, it is usr.txt.

  -P passw.txt: Specifies the path to a file containing a list of passwords. In this case, it is passw.txt.

  192.168.2.3: This is the IP address of the target system in this case.

  http-post-form "/admin/config.php: username=^USER^&password=^PASS^&command=login:Invalid Username or Password": This part defines the target web form and the parameters for the login attempt.

  - **/admin/config.php:** The path to the login page on the target website.
  - **username=^USER^&password=^PASS^&command=login**: This is the structure of the HTTP POST request for the login attempt. ^USER^ and ^PASS^

are placeholders that Hydra will replace with the usernames and passwords from the provided lists.
Invalid Username or Password: This is a string that Hydra will look for in the response to determine if the login attempt was unsuccessful. If this string is found, Hydra will consider the login as failed.