### 1. Introduction

The dynamic nature of cybersecurity necessitates ongoing awareness and proactive strategies to protect digital systems from emerging vulnerabilities and threats. **Penetration testing**, also known as **ethical hacking**, plays a crucial role in this effort by providing institutions with valuable insights into the strength and defenses of their security measures. By simulating real-world cyber-attacks, penetration testing evaluates the resilience of a system’s defenses, identifying potential weaknesses before malicious actors can exploit them.

### 1.1 Objective and Scope

There will be a network topology with different machines in it. This report details apenetrationtest conducted on the target system on the network **pWnOS**, with the primary goal of assessing its security posture. The test aims to:

* Identify security weaknesses through simulated attacks.
* Exploit vulnerabilities to demonstrate potential risks.
* Provide actionable remediation strategies.

The scenario assumes an **internal user compromise**, mimicking how attackers might infiltrate a system. The ultimate objective is exploiting my assigned target machine (pWnOS) and provide proof of exploration.

### 2. Summary and Recommendations

#### 2.1 Summary

The penetration testing process revealed several critical vulnerabilities within the **pWnOS** environment, exposing potential security risks. These issues spanned from weak authentication mechanisms to out-of-date software, both of which create loopholes for unauthorized privilege and system threat.

One predominant and concerning finding was the **lack of strong user access controls and weak authentication/password policies**, which posed a significant security risk. The Web interface, in particular, was not adequately protected by strong authentication methods or **Multi-Factor Authentication (MFA)**, making it vulnerable to unauthorized access. It suggested users use only letters, numbers and the underscore, and must be between 4 and 20 characters long. However, there was nothing enforcing these constraints as password such as “**test**” and “**kali**” were accepted during the pen testing. This highlights the need for **robust privilege/access control measures**, including MFA and strict password management practices, to enhance security.

Additionally, the presence of **exploitable vulnerabilities** in outdated system services, particularly on the **phpMyAdmin** was another major concern. These loopholes could be leveraged by attackers to gain access to sensitive data or compromise the system's integrity.

Another critical issue was the **absence of persistent security patches and updates**, which significantly weakened **pWnOS's** security posture. Failing to promptly deal with known vulnerabilities in a timely manner increases the risk of systems being successfully compromised by attackers, making the system more susceptible to threats.

#### 2.2 Recommendations

To enhance the security of **pWnOS**, the following measures should be implemented:

* **Consistent Patch Management**: Conduct **frequent security audits** and patch management to proactively identify and address weaknesses before they can be exploited. For example, the web server running on port 80 was running “http” which communicated in plain text, potentially revealing website exchange. This should be updated to use secure HTTP (https).
* **Strengthen Access Controls & Implement MFA**: Enforce strict access control policies and require **Multi-Factor Authentication (MFA)** for sensitive services to prevent unauthorized access.
* **Enhance Security Awareness Among Users**: Provide **ongoing cybersecurity training** to system users, emphasizing best practices such as locking screens, securing workstations, logging out remotely from all shells and turning off computers before leaving work to minimize security risks.
* **Enforce a Strong Password Policy**: Require passwords to be **10–12 characters long**, containing **both uppercase and lowercase letters**, at least **one special-case character, and a digit**. When combined with MFA, this will significantly reduce the likelihood of credential-based attacks.

### 3. Methodology

There are several recognized **penetration testing methodologies**, each providing structured guidelines for conducting security assessments. According to **Teaganne Finn of IBM (2024)**, the five most widely used methodologies include:

1. **Open-Source Security Testing Methodology Manual (OSSTMM)**
2. **Information System Security Assessment Framework (OISSG)**
3. **Open Web Application Security Project (OWASP)**
4. **National Institute of Standards and Technology (NIST)**
5. **Penetration**  **Testing Execution Standard (PTES)**

For this penetration test, the **OSSTMM methodology** was selected due to its **scientific approach** and adaptability. This methodology provides well-structured, accessible guidelines for testers, ensuring a thorough and systematic assessment.

The specific approach followed in this assessment includes:

1. **Information Gathering** – Collecting details about the target system to identify potential entry points.
2. **Scanning and Mapping** – Analyzing the network structure and identifying active hosts.
3. **Enumeration** – Extracting information about services, users, and configurations.
4. **Gaining Access** – Exploiting vulnerabilities to penetrate the system.

This structured methodology ensures a comprehensive evaluation of **pWnOS's** security weaknesses, helping to identify and mitigate risks effectively.

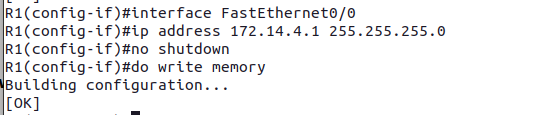
### 4. Network Design and Topology

The network environment was established within the Apporto virtual lab platform, adhering to the specified architecture outlined in the setup guide. The topology consisted of a Windows VM, a Kali Linux machine, a Switch, a Cisco 7200 series router, and a pWnOS vulnerable system — a common setup in penetration testing labs designed to simulate real-world attack and defense scenarios.

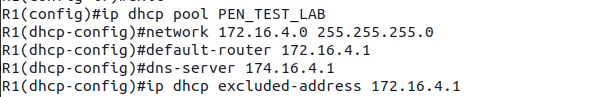
The Cisco 7200 router was configured to serve as the DHCP (Dynamic Host Configuration Protocol) server, dynamically assigning IP addresses to connected hosts within the 172.16.4.0/24 subnet as seen below:

**Configuring Terminal and setting up the interface of the router**





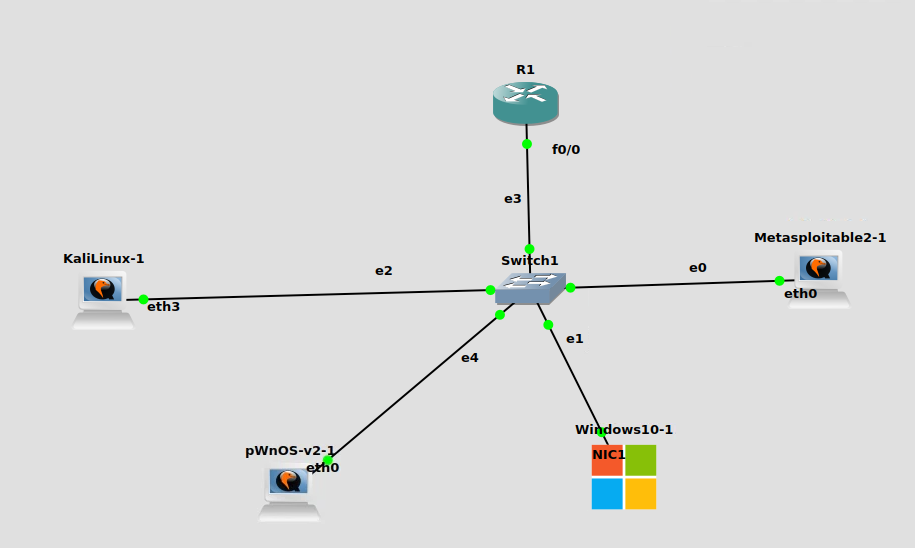
**Configuring the DCHP on the router**



This setup not only ensures centralized IP address management but also mirrors enterprise-grade infrastructure often targeted in reconnaissance and exploitation phases of penetration testing.

By integrating both offensive (Kali Linux) and defensive or vulnerable (Windows and pWnOS) systems within a controlled virtual network, the environment provides a robust framework for practicing key cybersecurity techniques. These include network scanning, enumeration, vulnerability analysis, and exploitation, all of which are fundamental components in ethical hacking methodologies such as those outlined by the **OSSTMM** methodology explained above.

**Final network design and set up**



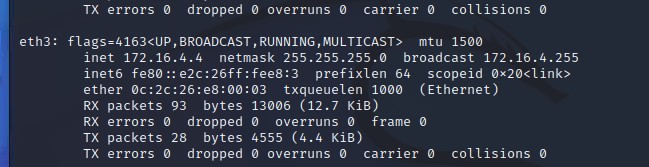
Switch information:



|  |  |
| --- | --- |
| All Devices in the network and their mac addresses | |
| Windows | 0c:8e:c2:06:00:00 |
| pWnOS | 0c:1a:1a:87:00:00 |
| Metasploitable | 0c:fc:57:b2:00:00 |

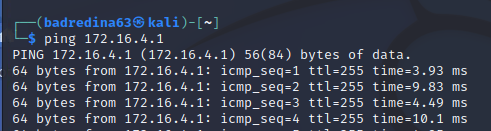
### 5. Information Gathering

With the network topology done, the tester set up the kali machine to be used as the attacking VM, by creating and configuring the user as **badredina63**. The first thing the tester did was verify if the router and network is set up properly and actively running. To do this, the IP of the target machine (kali) was checked with the command **ifconfig**, and it showed **172.16.4.3** as expected because from the network diagram, it was configured on **eth3** to the switch.

**Verify on kali**  
   


Now, to test if the DHCP server is up, a ping was used which successfully received messages from the router. This successful communication suggests that the DHCP server component on the router is likely up and functioning as expected. While ping does not directly test DHCP functionality, the positive response confirms that the router is online, which is a good preliminary indication before performing more specific DHCP tests.

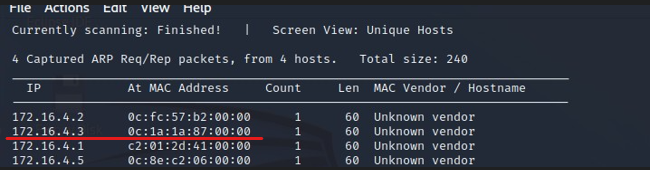
**Responses from the serve**r:



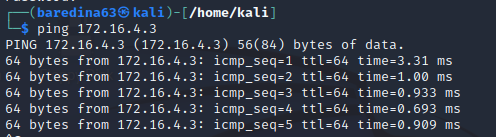
With the preliminary verification above confirmed, it is time to discover the machines in the network to find the target. The command below was used to achieve this:

Table 1 (discovering IPs in the network)

|  |
| --- |
| sudo netdiscover -r 172.16.4.0/24 |

The **netdiscover** command requires superuser (**sudo**) permissions to grant privilege to network associated information that normal users are not permitted to. “**netdiscover**” is a CLI (Command Line Utility) that comes with kali to discover all devices on the network. The -r flag details the range of IP addresses configured on the network (172.16.4.0/24). The figure below shows the result after executing the command above:  
   


After the tabular list from the result, the reporter identified the target as the machine with MAC address as **0c:1a:1a:87:00:00** and IP address as **172.16.4.3**. To verify if this is reachable, a **ping** was done which confirmed it is up as seen below:

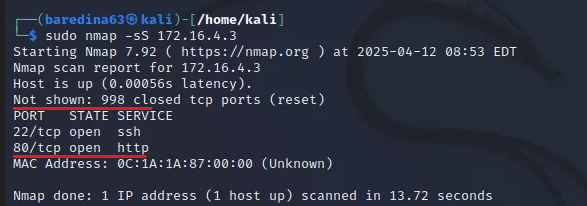


With this discovery, the next step was to collect information about the target machine. The aim is to remain unknown and stealth in collection the information about the device on the network so as to reduce any traces and suspicions on the firewalls. To achieve this, nmap command was used with the flag “-sS”, which ensures low profile and stealthiness.

Table 2 (being stealth in gathering info)

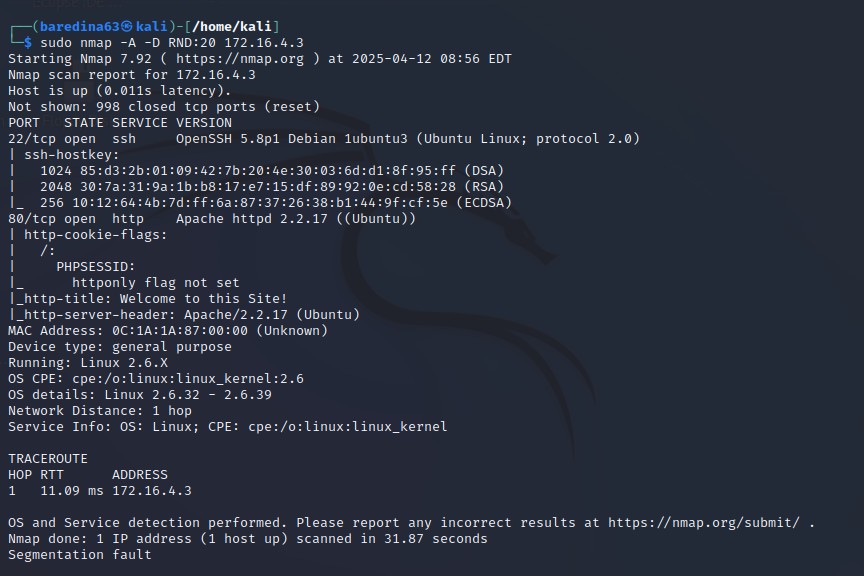
|  |
| --- |
| sudo nmap -sS 172.16.4.3 |

The command shows opened ports running on the target VM.



Nonetheless, collection information about opened and running ports is not enough, more information such as ssh-host key information, authentication level and operation system is needed about the target. To achieve this, the -A flag is used in combination with nmap. To additionally achieve non-suspicions and quietness in the network, 20 random IP addresses were spawned which will act as a decoy, making it much harder to reveal the actual IP address collecting the information. The command **-D RND:100** was used to achieve this.   
  
Table 3 (detailed information)

|  |
| --- |
| sudo nmap -A -D RND:20 172.16.4.3 |

The result of this is presented below:  
   
  
The table below is a summary of the target machine:

|  |  |
| --- | --- |
| Target VM Details : pWnOS | |
| IP Address | 172.16.4.3 |
| Operating System | Linux 2.6.x (kernel 2.6.32 – 2.6.39), Ubuntu Linux |
| Host status | |  | | --- | |  | | Host is up (0.011s latency) | |
| Traceroute | 1 hop, 11.09 ms to 172.16.4.3 |
| Opened Ports | 22 (SSH), 80 (HTTP) |
| Ssh-host key info: | 1. DSA: 85:d3:2b:01:09:42:7b:20:4e:30:03:6d:d1:8f:95:ff 2. RSA: 30:7a:31:98:17:e7:15:df:89:92:0e:cd:58:28 3. ECDSA: 10:12:64:4b:7d:ff:6a:87:37:26:38:b1:44:9f:cf:5e  |  | | --- | |  | |

### 6. Scanning and Mapping

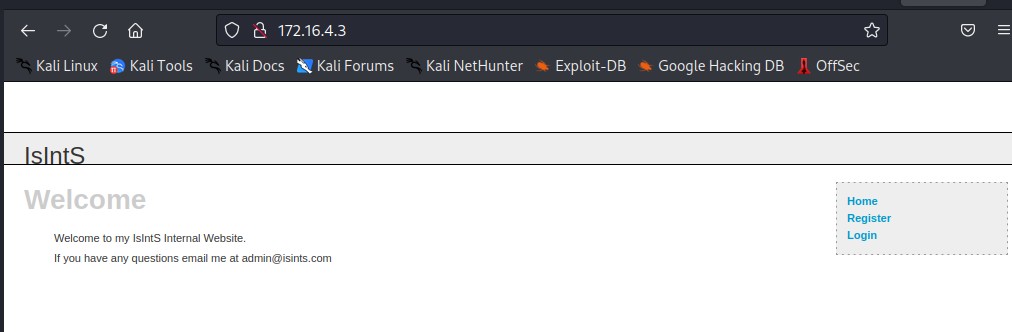
During the information gathering phase, a full TCP scan was executed using Nmap to identify open ports and services running on the target system. The scan revealed the following:

* **Port 80/tcp** – Open
  + **Service**: HTTP
  + **Web Server**: Apache HTTPD 2.2.17
  + **Operating System**: Linux (Debian-based as suggested by the Apache version and headers)
* **Port 22** (ssh).

**Initial Web Interface Exploration – Port 80 scan**

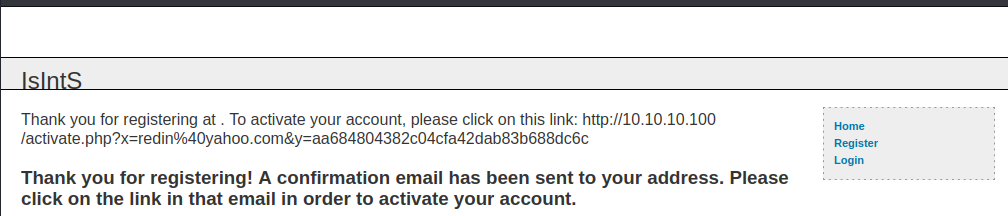
The presence of an open port 80 indicates that an HTTP server is active. Since HTTP is associated with web services, the tester used Kali’s inbuilt Firefox web browser to scan and gather additional information.

The homepage of the web server displayed the message **"Welcome to my IsIntS Internal Website, If you have any questions email me at** [**admin@isints.com**](mailto:admin@isints.com)**!" as shown** in the figure below.

  
The email **admin@isints.com** on the homepage instantly looked suspicious as it indicates the admin email and if I discover the password for that email, I will have admin privileges when I login.  
  
On the far-right side of the homepage displayed buttons for” Home, Register, and Login”. These suggested the port 80 is running a user login portal for a web application or service and involves user account management.

I navigated to the login page, entered the email address as **admin@isints.com** and tried some common passwords like *admin*, *root*, *pasword123, 1==1,* and more but none of them worked.

I tried to register an account using the credentials: email: [redin@yahoo.com](mailto:redin@gmail.com)” and password as “kali”. After clicking the register button, the page below was shown:



I checked the email but noticed there was no link in it to activate the account. I then discovered that the activation link had the following key findings:

* The activation URL comprised two GET parameters:
  + x: The email address (URL-encoded)
  + y: A hash or token value, possibly used to validate the account

### **Observations and Implications**

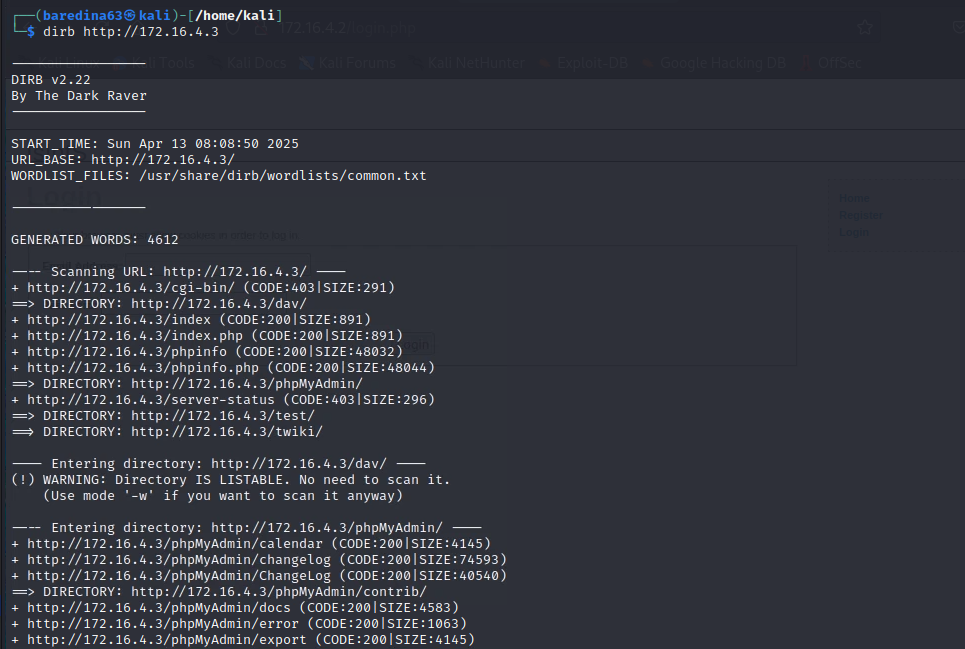
1. **Static or Predictable Token Format**:  
    The structure of the token (y) appears consistent across different registrations, and it is likely derived using a hash function. This indicates the possibility of:
   1. **Token prediction or forgery**, especially if a weak hashing algorithm like MD5 is in use.
   2. A **lack of proper salting** or use of easily guessable salts (e.g., email + static string).
2. **No Email Verification in Practice**:  
    The application directly shows the activation link after registration, bypassing the need to access an actual email inbox. This opens the application to **automated account creation** and **spam attacks**.

Furthermore, after noticing that there were pages like **register.php**, **index1.php**, and **login**.**php**, the tester realised there might be other existing pages within the website and could be scanned and accessed. To explore these pages, the command shown in Table 5 was executed.

Table 3 (exploring pages)

|  |
| --- |
| dirb [http://172.16.4.3/](http://172.16.4.2/) |

Dirb is a web content enumeration and discovery tool that conducts directory brute-forcing to identify hidden directories and files on a web server (Reff, 2017). The outcome of this process is shown below.



These discoveries are vital because revealing the presence of a **phpMyAdmin** installation (<http://172.16.4.3/phpMyAdmin/>) is a critical finding, as **phpMyAdmin** is a widely used web-based database administration tool for MySQL and MariaDB. If improperly secured, it can serve as a high-value target for exploitation.  
  
The important pages discovered by performing the DIRB scan will be dealt with in detail under the enumeration section of the report.

**Port 22scan**

Port **22** is running the **Secure Shell (SSH) protocol**, a critical service commonly used for **secure remote administration** of networked systems. This suggests that the user may have **remotely accessed their organization’s internal systems** to perform administrative tasks, such as **system configuration, troubleshooting, or software management**. Additionally, SSH is often leveraged for **secure file transfers (SFTP/SCP), remote command execution, and even tunneling other services** like printer or fax sharing across networks.

For a penetration tester, the presence of an **open SSH service (port 22)** presents a **valuable attack surface**, as improperly secured SSH servers can be exploited to **gain unauthorized access, escalate privileges, or pivot deeper into the network**. Common attack vectors include:

* **Brute-force attacks** against weak passwords.
* **Exploiting outdated SSH versions** with known vulnerabilities.
* **Abusing misconfigured key-based authentication** (e.g., weak or exposed private keys).
* **Session hijacking** if encryption is compromised.

If the tester can **compromise SSH credentials** (via phishing, leaks, or brute-forcing), they may gain **direct shell access** to the system, allowing **lateral movement, data exfiltration, or persistent backdoor installation**. Therefore, securing SSH with **strong passwords, key-based auth, fail2ban, and firewall restrictions** is essential for mitigating these risks.

### 7. Enumeration

At this stage, the testing requires proactively querying systems and services on the target to collect information, including shared resources, user accounts, file systems, and configurations, following the scanning and mapping process.

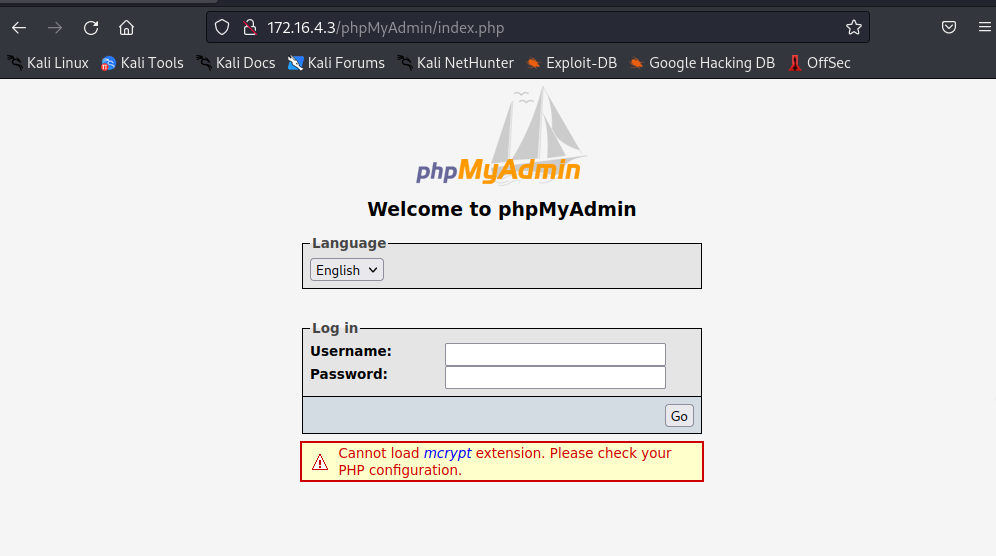
During the mapping and scanning phase, it was identified that there are paths like **phpMyAdmin.php** that can be explored.

**Directory Enumeration**

The scanning stage using DIRB exposed several accessible endpoints such as, ***phpMyAdmin/changelog***, ***phpMyAdmin/config, phpMyAdmin***/***import***, ***phpMyAdmin/export***, and more. I checked all these endpoints for clues and the results are:

**A. phpMyAdmin Dashboard (**/phpMyAdmin/index.php**)**

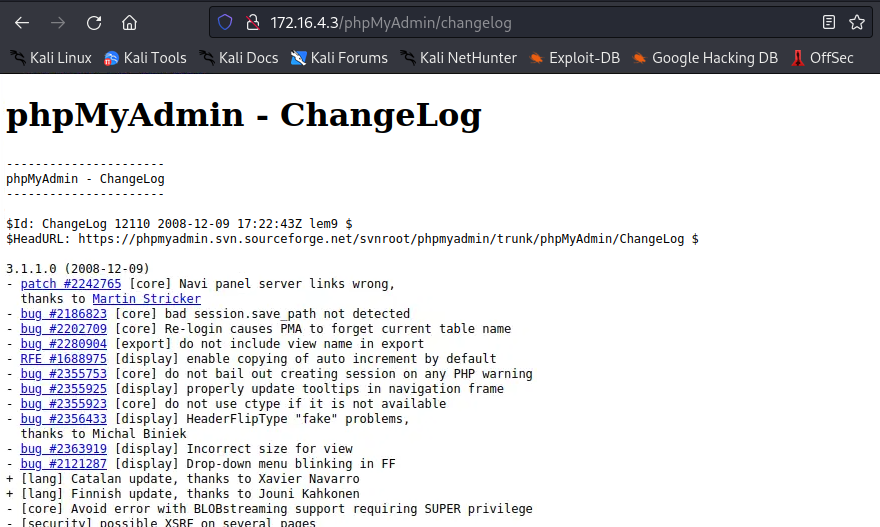
* **Status Code:** 200 OK
* **Significance:**
  + The main login page for phpMyAdmin.



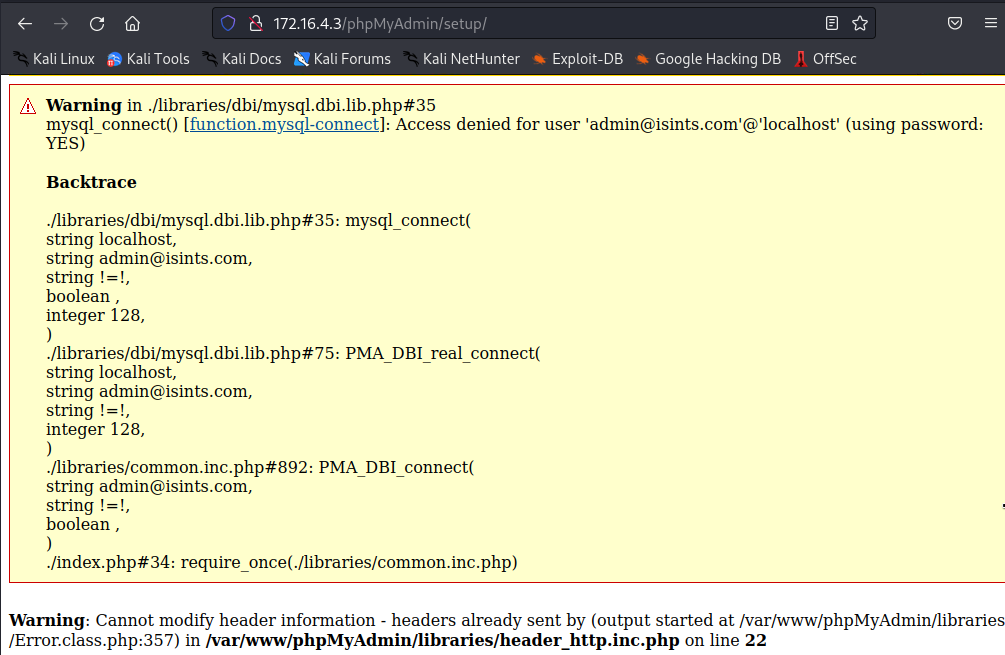
With this, I tried some common default credentials with username and password values as **root: root, admin: admin**, and even blank passwords but nothing worked.

If any of these attempts were successful logins, then the tester would have grants to full database access, allowing **SQL injection, data exfiltration, or even remote code execution** via SQL queries, but unfortunately, that did not work.  
  
**B. Version and Changelog Files (**/phpMyAdmin/Changelog**,** /phpMyAdmin/changelog**)**

* **Status Code:** 200 OK
* **Significance:** Reveals the **phpMyAdmin version**, which can be cross-referenced with known vulnerabilities (e.g., CVE-2018-12613 for local file inclusion).

  
The tester tried several links on this page but nothing suspicious occurred.  
  
**C. Configuration and Setup Directories *(/phpMyAdmin/setup/*)**

* **Status Code:** 200 OK (if accessible)
* **Significance:** The **/setup/** directory may contain **configuration scripts** that could leak credentials or allow unauthorized changes.

When the tester navigated to the ***(/phpMyAdmin/setup)*** page, the screen below was shown:  


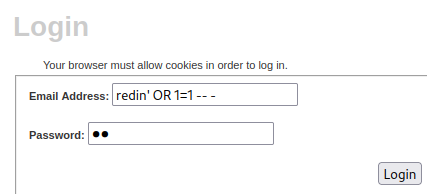
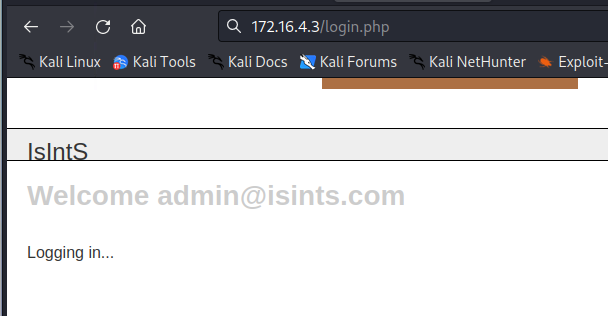
This is interesting because it shows the warning and stack trace of when the tester tried to log in using the admin email and random passwords. The tester did aadditional research, and according to Tim Fisher (2023), web pages displaying error messages might be susceptible to vulnerabilities such as **Path Traversal, SQL Injection, and File Inclusion**. These potential risks will be explored in trying to gain access in Gaining Access section of the report.

### 8. Gaining Access.

This pen-testing phase focuses on exploiting the vulnerabilities identified during the previous stages and using them to obtain access to the target.

The idea here was to find ways to obtain access to the system. From the enumeration stage above, the stack trace on the ***myPhpAdmin/setup*** implies the system may be vulnerable to SQL injection. Hence, the tester returned to the login page, and tried the infamous **UNION SELECT** SQL injection. This approach is frequently used by penetration testers and attackers to manipulate SQL queries and extract sensitive information from a database.

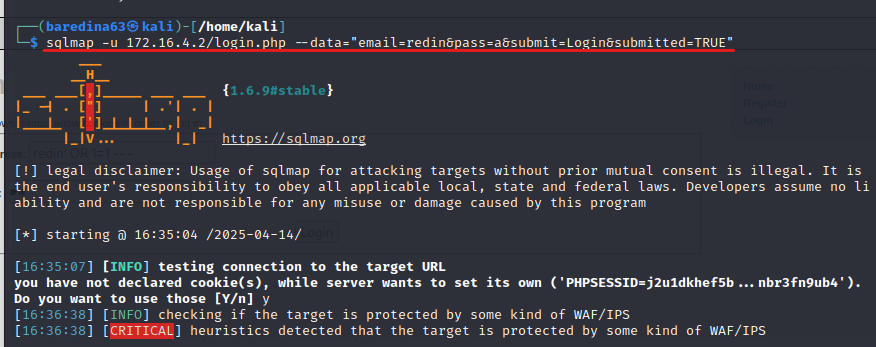
The UNION SELECT technique works by injecting a crafted SQL statement into an input field (like a username or password box in this case), with the goal of combining the results of two queries into a single result set. If the application fails to properly sanitize or validate user input, the injected UNION SELECT query can trick the database into revealing additional data — often from unrelated tables.

With this, I tried the query **redin’ OR 1=1-- -** and a random password “12” as seen below:  
  
  
  
The confirmed the suspicious of the SQL injection vulnerability as it showed the results below:  
  


However, after this, nothing else happened. I tried refreshing the page but that did not work either.

To assess the login page for SQL injection vulnerabilities, the tool **sqlmap** was utilized with the following command:

|  |
| --- |
| sqlmap -u http://172.16.4.2/login.php --data="email=redin&pass=a&submit=Login&submitted=TRUE" |



Upon running this test, **sqlmap** returned several critical observations:

* The target was identified to be running **MySQL** database version ≥ 5.0.12.
* The **email** parameter was found to be **vulnerable to SQL injection**, specifically:
  + **Error-based injection** using FLOOR function.
  + **Time-based blind injection** using SLEEP.
  + **UNION-based injection** was also tested and confirmed to be applicable.

These results confirmed that the login form is highly susceptible to SQL injection, allowing unauthorized queries to be injected and executed against the backend database. The image below shows the vulnerabilities that were identified.

A screenshot of a computer program

AI-generated content may be incorrect.

Additionally, **sqlmap** identified that the server set its own cookies ('PHPSESSTD') and the target was protected by some kind of WAF/IPS (Web Application Firewall/Intrusion Prevention System), which necessitates the stealthiness in carrying out the pen-testing to avoid leaving traces behind.

**Credential Extraction.**

After confirming the SQL injection vulnerability, the tester proceeded to enumerate the database structure:

1. The sqlmap tool automatically extended its testing range when it detected UNION query injection was possible
2. The 'ORDER BY' technique was used to efficiently determine the number of columns (8) in the query
3. Afterwards, it fetched the data corresponding to each column which showed the email, first\_name, last\_name, password hashes and more as shown below:

A screen shot of a computer

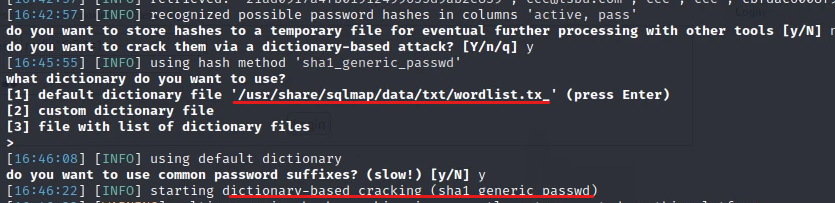
AI-generated content may be incorrect.

It then retrieved a user table containing **hashed passwords**, as shown in the output

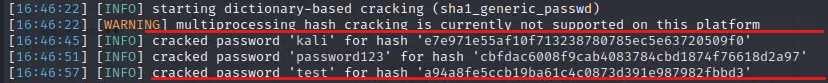
A screenshot of a computer program

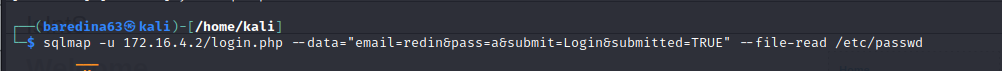
AI-generated content may be incorrect.

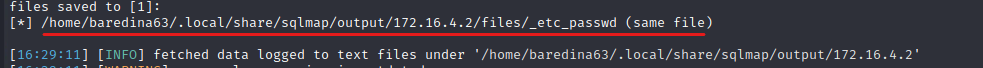
Sqlmap then provided the option to store the hashes and attempt to crack them using its own wordlist (/usr/share/sqlmap/data/txt/wordlist.tx\_) for **dictionary-based attack** as seen below:

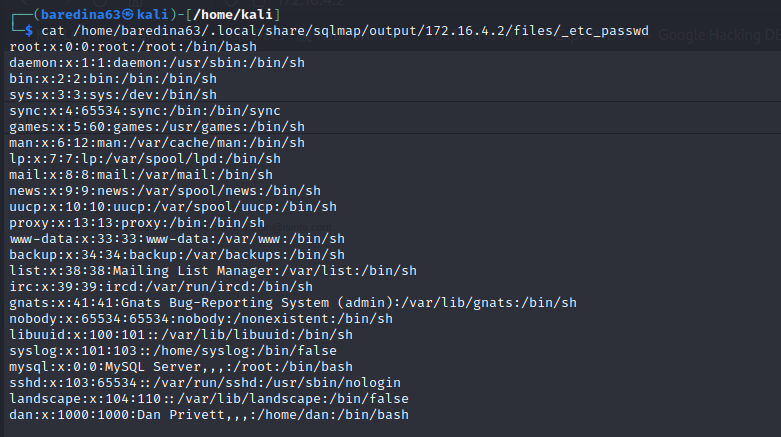


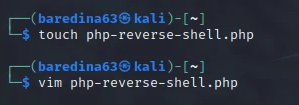
After running the dictionary attack, the hash type was auto detected as **SHA1 (sha1\_generic\_passwd)**. This process successfully recovered plaintext credentials of user password from the database as seen below:

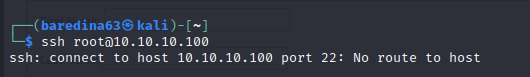
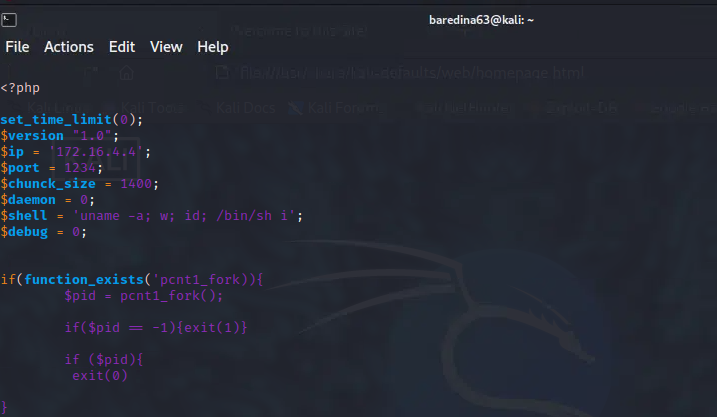


However, these are the password credentials the tester used when testing the “register” page under scanning and mapping. The actual password for the email [**admin@isints.com**](mailto:admin@isints.com)was not revealed**.**  
  










### 9. Conclusion

Penetration testing is essential for proactively identifying and mitigating security vulnerabilities before malicious actors can exploit them, ensuring robust defense mechanisms for organizational systems. This assessment underscores the critical need for regular security audits, strong access controls, and timely patching to safeguard against evolving cyber threats.