# Penetration Test Initial Assessment Template

## Reconnaissance

* Describe the methodology and process you used to perform research and recon on the target (at least one paragraph and screenshots)

As both OS are in the same network, use ifcoonfig and nmap to find the target. So it is 172.16.202.9 with http and ssh open. Ubuntu System.

Text

Description automatically generated

Google zico, it you can see that root user can be compromised

Graphical user interface, website

Description automatically generated

## Scanning / Enumeration

* Describe the scanning and enumeration you performed against the target
* (at least one paragraph and screenshots)

Use nmap with in depth scan and nikto to see the open port, system info, and system’s vulnerability.

Text

Description automatically generated

## Gaining Access

* How did you gain access?

As we see in the scanning test, many directories are open to exploits, so we use dirbuster. To find the admin directory to access the website

Table

Description automatically generated

We find the tesd\_db.php

A screenshot of a computer

Description automatically generated with medium confidence

## Maintaining Access

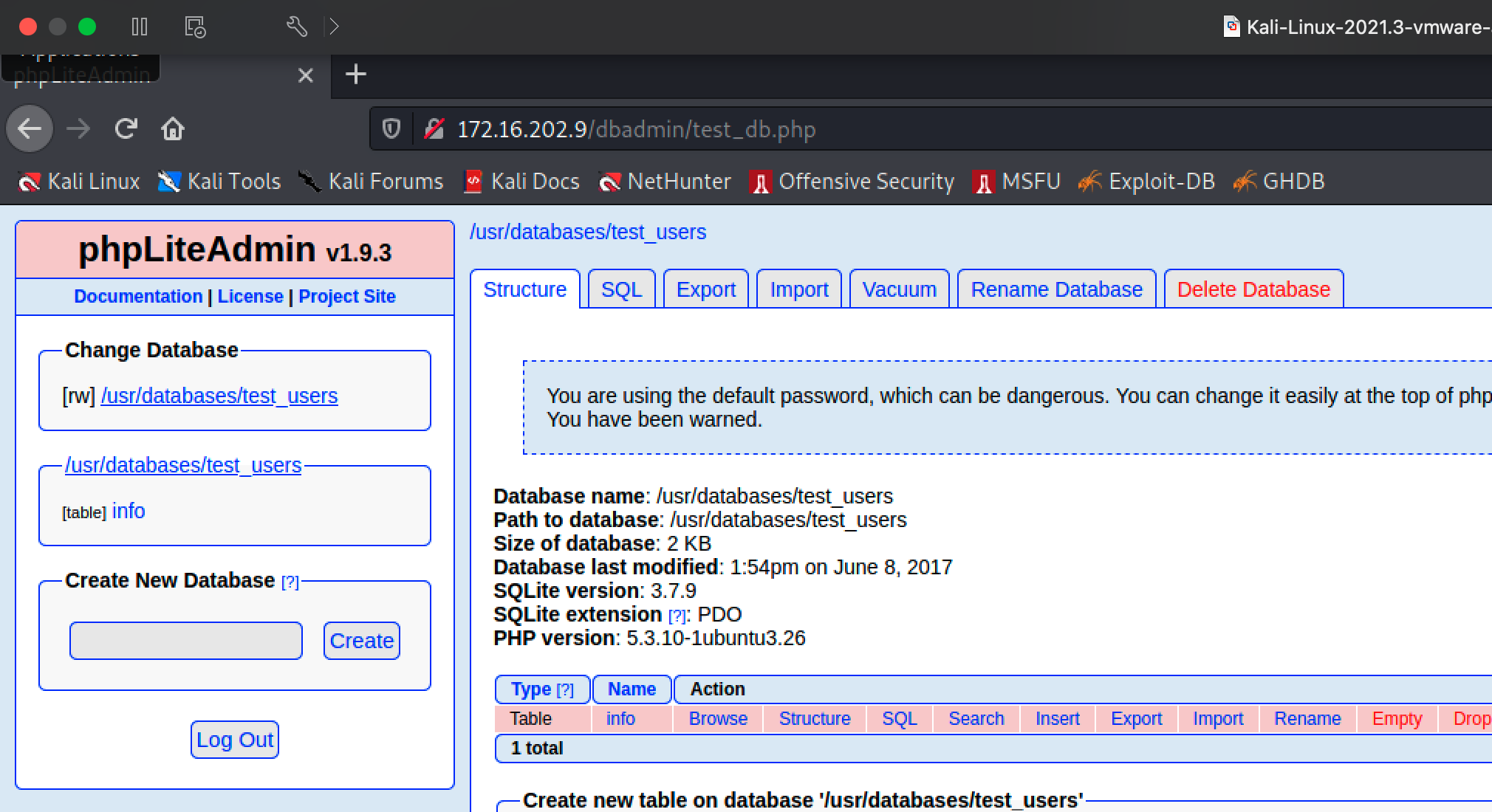
* What did you do to be persistent on the target host?

we can use durp suites to try the find the hash. And we find the PHPSSID hash

Graphical user interface, text, application

Description automatically generated

We tried the md5 hash to find out the password is “admin” and gain access to the database



## Covering Tracks

* What steps did you take to remove the evidence you were there?
* Use private windows to access the website and renew the dhclient.
* A screenshot of a computer

  Description automatically generated with medium confidence

## Summary

* Describe what you learned during the course of your attack

I learn that we can use the old ways to gain access the websites, such as using possible password and hash to find out the possibilities.

First – you need to know the possible ways to gain access, using source like nmap, nikto, and google. Somehow people can access to root but I could not. Using the birbuster and acquires multiple wordlists to find the possible directories available.

Second – using the old ways to gain access, use man-in-the-middle to find the hash, and rainbow hash it using the wordlist.

Third – after multiple tests of finding the hash, and decrypt the hash. Finally gain the access. And use the traditional ways to covering tracks using deleting cookies, private windows, and killing process, and renew the ip / mac address of the vm.