**Prepared by: Rose Wairimu Macharia**

**For: Kratikal Academy**

**Report content: Detailed Boot to Root Report**

**Status: Completed**

**Date: 18th February 2021**

**Scope**

The penetration test was conducted to find and exploit the vulnerabilities in the Kioptrix Level 1.3 (#4) VM and capture the flags within the virtual machine.

My main objective was to gain the root access via any means possible.

The aim to carry out the test was to identify the steps and methods that an attacker could probably use to gain access to the victim. The test was also done to evaluate the level of risk to the victim and finally to identify recommendations that could be used to prevent search kind of attacks.

The results of this Security Testing can be used to enhance the security feature of Kioptrix Level 1.3(#4).

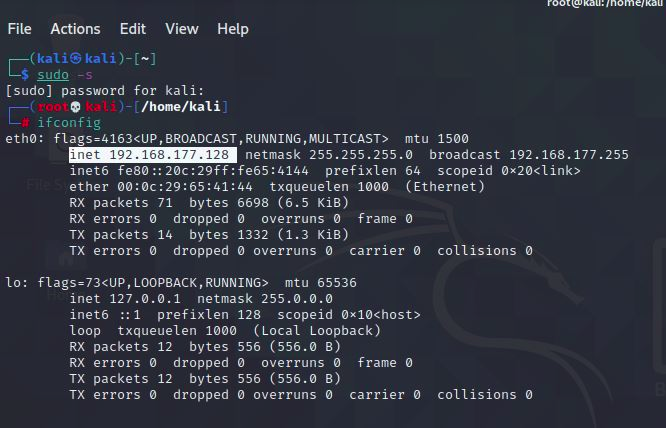
**Approach**

The test I conducted was a black box test since there was no technical and functional information given to me that I could work with. The test cases generated are based on knowledge acquired from my web application lectures and this is a way to gain the experience needed in a penetration testing field.

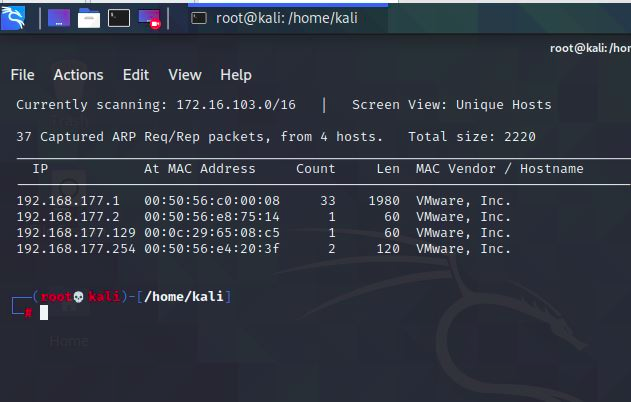
The setup consisted of a Local Area Network (LAN), Kali Linux attacker virtual machine and the victim virtual machine Kioprix level 4.

**Summary of results**

IP Address of the attacker VM: 192.168.177.128



Identified address of the victim machine VM: 192.168.177.129

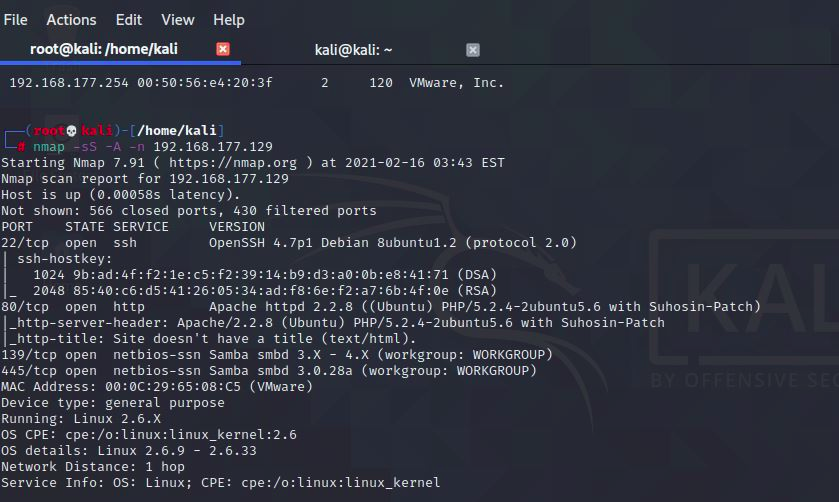


Initial scan of the network using the (ifconfig) command resulted in the discovery of the attackers IP address. Then carried a discovery command (net discover -i eth0) to identify the IP address of the victim machine. With the information above lead to the discovery of open ports by use of Nmap IP scan (). The following ports were discovered:

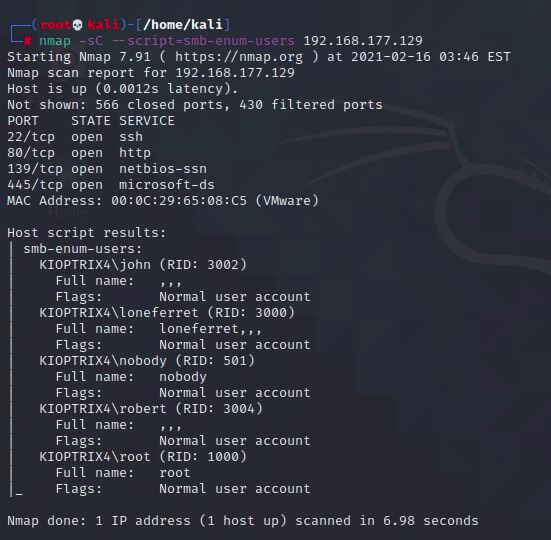
22/tcp – Service is running with version OpenSSH

80/tcp – HTTP service is running with version Apache httpd 2.2.8

139/445tcp – NetBIOS-SSN: The NetBIOS service is open so it can easily enumerate SMB for any public facing sharing as well as usernames



Since port 22 is open, one can easily enumerate the usernames through NetBIOS with the help of Nmap command (Nmap -sC -script=smb-enum-users 192.168.177.129)



We see that there are five usernames discovered

1. john

2. Loneferret

3. Nobody

4. Robert

5. root

For vulnerability check; use Nikto which is an open source vulnerability scanner.

It appears that the Apache/2.2.8 is outdated

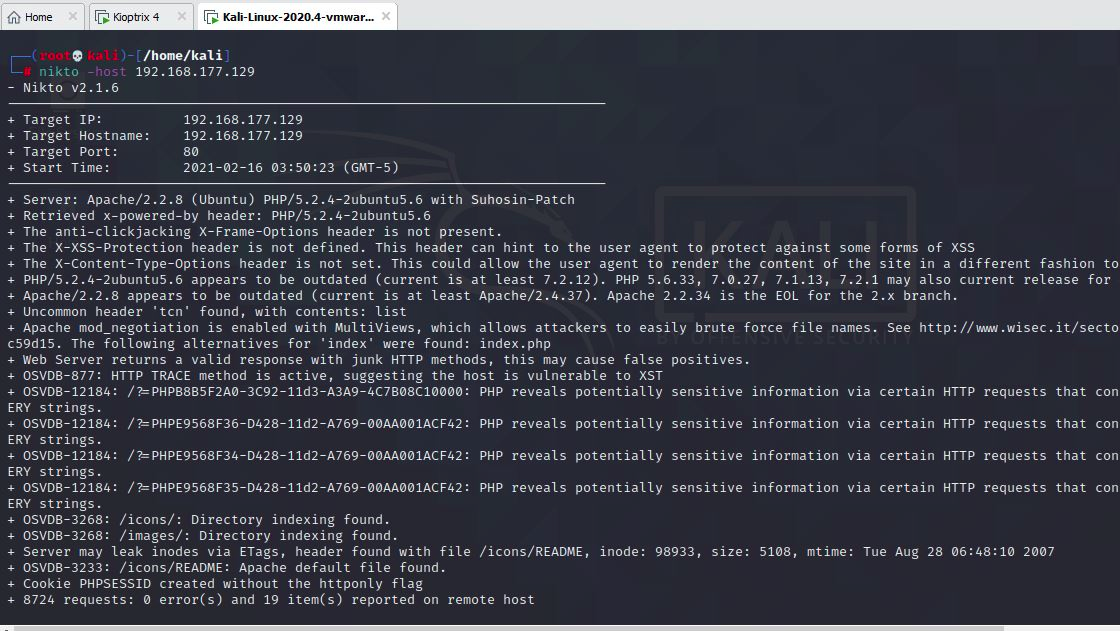
PHP reveals potential sensitive information via certain HTTP requests

there certain directories indexing found.

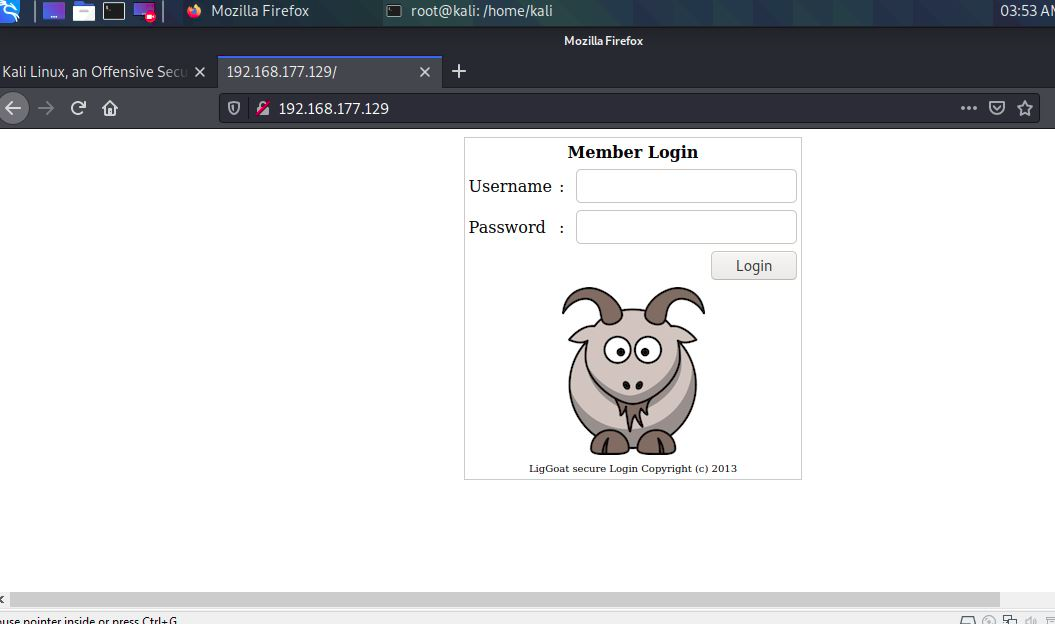
PHPSESSID created without the HTTP only flag

The anti-clickjacking X- Frame-options header is not present.

This are just some of the vulnerabilities collected by Nikto

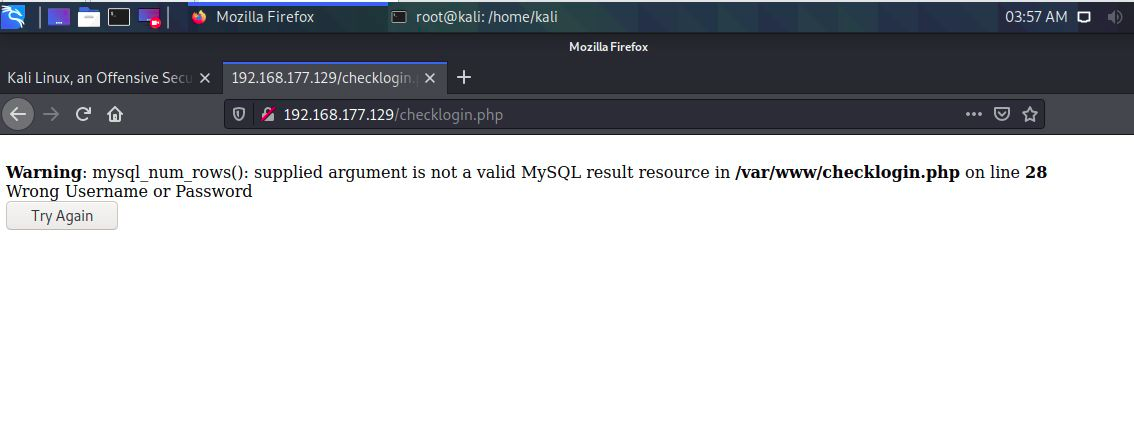
****

Noticed that port 80 is open, so try opening the ip address in the browser. It opens giving us a login page

****

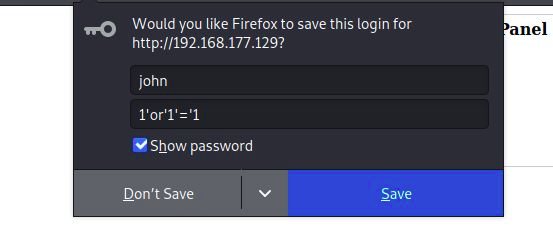
With this we can check if its vulnerable to SQL Injections by tampering with the username and password position, this by adding an illegal character (‘)

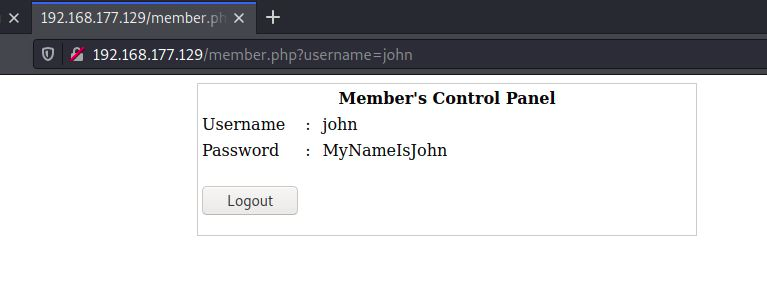
the login page returns an error that tells that the page is vulnerable to blind based sql injections

****

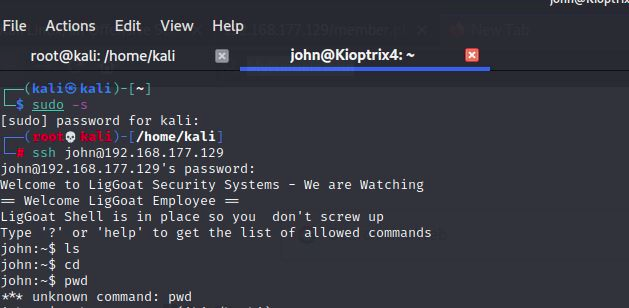
In blind based sql injections you can inject the login in page with a Boolean statement to see the output of the page.

Example: 1’or’1’=’1 which returns a true value

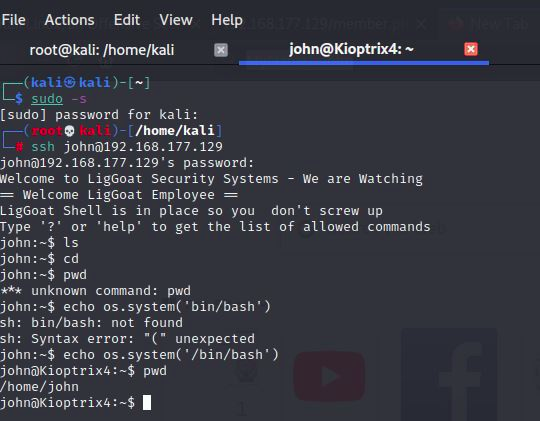
****

****

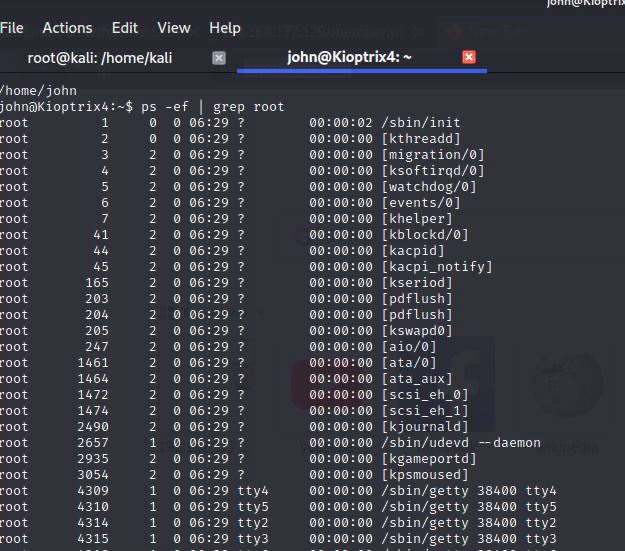
With john’s password one can try to do SSH by ([sshjohn@192.168.177.129](mailto:sshjohn@192.168.177.129))

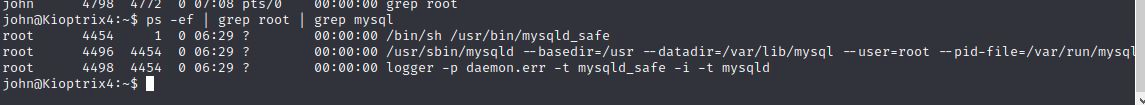
the shell is limited to certain commands which are ls and cd. Pwd seems unknown

With the command (echo os. system(‘/bin/bash’)) one can bypass the limited shell. The pwd command gives us more access to the current working directory.

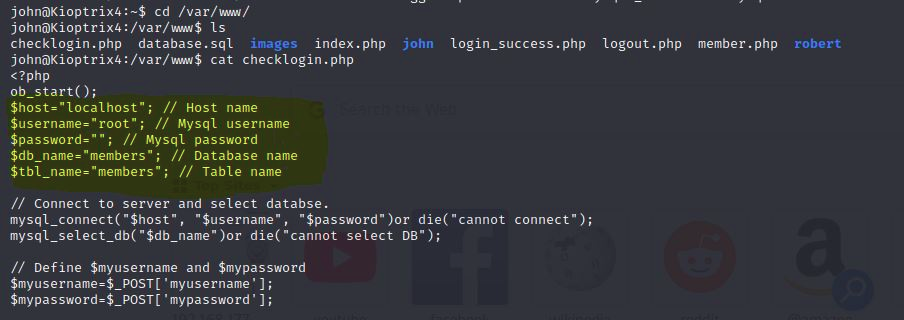
****

Access the root processes by use of grep. Check if MySQL is running or not by running the command (ps -ef | grep root | grep MySQL)





MySQL is running by root user this means one can easily carry out privilege escalation with MySQL user defined functions. The MySQL provides one with the database username and also password details in a file located at var/www/directory. The MySQL has no password so it’s easy to bypass MySQL with user defined functions

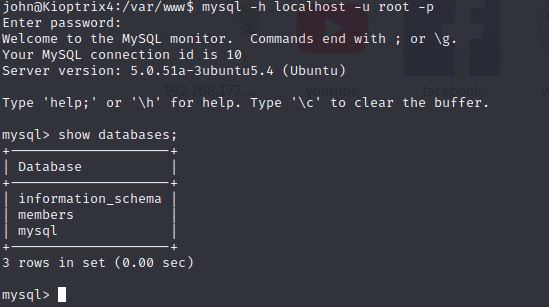


You can directly access the database with MySQL client. This gives you the following databases

information schema

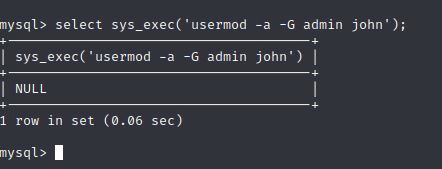
members

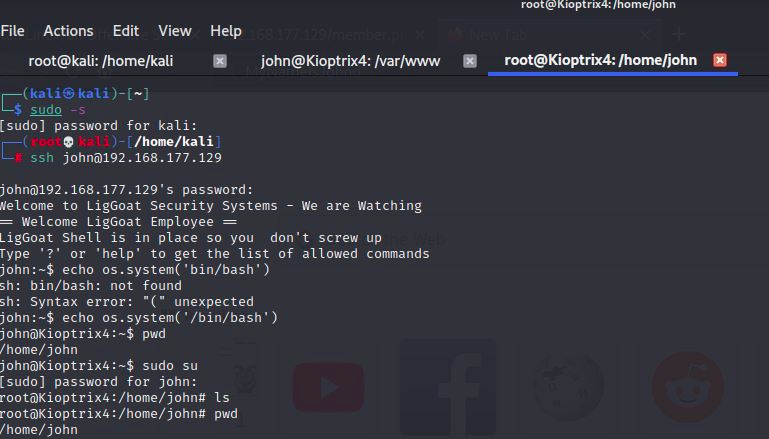
MySQL



Show databases; gives a list of the databases in the target IP

John one of the usernames can be changed to have admin privileges by use of the sys\_exec. This will enable usermod to run and give john the admin privileges.





Rating of the vulnerability Is **High**

**Impact:** The kioptrix VM contains a number of outdated services running. The vulnerabilities allow the attacker to gain unauthorized access to the system. The victim has a local privilege escalation which is easy to leverage and tamper with the externally exposed host entirely

**Recommendation**

Virtual Machine is just a representation of the actual system. All services should be up to date to avoid being exploited. This can be achieved by the use of open source software which provide an overview of all loopholes and also can be used to patch the flaws.