Everything you wanted to know about mainframe security, pen testing and vulnerability scanning .. But were too afraid to ask!

Mark Wilson

markw@rsmpartners.com

Session Details: Footprinting

Agenda

IBM Mainframe
Are they really secure?

- Introduction
- Top Ten Audit Issues Seen
- Footprinting
- How do you protect yourself?
- Questions

Introduction

Introduction

- Mark Wilson
  - Technical Director at RSM Partners
  - I am a mainframe technician with some knowledge of Mainframe Security
  - I have been doing this for over 30 years (34 to be precise ☺)
  - This is part two of seven hour long sessions on mainframe security
  - Full details can be seen on the New Era Website:
    - http://www.newera-info.com/New.html

Where's Home?


The outer Islands
Scotland (North)
Scotland (South)
North East
North West
Northern Ireland
Yorkshire & the Humber
East Midlands
West Midlands
Eastern Region
Wales
London
South East
South West

Language!

- And I don’t mean bad language!

- UK and USA …… two countries separated by a common language!

- When is a ZEE not a ZEE?
- When it’s a ZED

- What is PARMLIB(e)?
- When its PARMLIB

What's this?

- Zeeeebra?
- No it’s a Zebra!
- Hopefully this will help you understand me ☺

Objectives

- These sessions will give you an insight into what can happen to your system when you think you have it all covered
- The information is shared for your use and your use only to enhance the security of the systems you manage
- The information being shared is sensitive information and if in the wrong hands could do serious damage
- Hopefully I will show you that there is more to security than just a security product such as RACF, ACF2 and TSS!

Top Ten Audit Issues Seen

Top Ten Audit Issues Seen

- I missed this of the initial session and I have been asked to cover it here ☺
- This is my view of the most common and simple issues we see at the majority of mainframe security implementations
- Whilst I use RACF language they are just as applicable to ACF2 and Top Secret

Top Ten Audit Issues Seen

- Userid Based

1. Userids with NO Password Interval
2. Excessive Userids with the OPERATIONS or SPECIAL Attributes
3. Inappropriate Usage of Superuser Privilege, UID(0)
4. Started Task Userids that are not Defined as PROTECTED
5. Userids with default passwords

Top Ten Audit Issues Seen

- Dataset & Resource Access

1. Excessive Access to APF Libraries
2. Production Batch Jobs have Excessive Dataset & Resource Access
3. Dataset and General Resource Profiles in WARNING Mode
4. General Resource and Dataset Profiles with UACC of READ or Higher
5. Improper Use or Lack of UNIXPRIV Profiles

And remember….

- The majority of issues seen come from the knowledgeable and privileged insider!
- We rarely see issues where a mainframe is compromised from outside of the network…..
- But it doesn’t mean it wont or has not happened before

Footprinting

Footprint the system

- Document the current system configuration
- This is referred to as “Footprinting” the system
- This will allow us to probe the system in a controlled manner
- We will discuss the tools, commands & datasets/parameters that can be used to accomplish z/OS Footprinting

Hints & Tips

- Mos
  REA
- We ckers
- Its v g of this
  data
- But

```
struct group_info init_groups = { .usage = ATOMIC_INIT(2) };
struct group_info *groups_alloc(int gidsetsize){
    struct group_info *group_info;
    int nblocks;
    int i;

    nblocks = (gidsetsize + NGROUPS_PER_BLOCK - 1) / NGROUPS_PER_BLOCK;
    /* Make sure we always allocate at least one indirect block pointer */
    nblocks = nblocks ? : 1;
    group_info = kmalloc(sizeof(*group_info) + nblocks*sizeof(gid_t *), GFP_USER);
    if

    gro
    gro
    ato

    if (gidsetsize <= NGROUPS_SMALL)
        group_info->blocks[0] = group_info->small_block;
    else {
        for (i = 0; i < nblocks; i++) {
            gid_t *b;
            b = (void *)__get_free_page(GFP_USER);
            if (!b)
                goto out_undo_partial_alloc;
            group_info->blocks[i] = b;
```

ACCESS DENIED

TSO Access

- Required for the majority of tasks

```
 Menu  Utilities  Compilers  Options  Status  Help
 ------------------------------------------------------------------------
                         ISPF Primary Option Menu
Option ===>  _
                                                                         
0  Settings      Terminal and user parameters          User ID . : TSGMW
1  View          Display source data or listings       Time. . . : 03:29
2  Edit          Create or change source data          Terminal. : 3278
3  Utilities     Perform utility functions             Screen. . : 1
4  Foreground    Interactive language processing       Language. : ENGLISH
5  Batch         Submit job for language processing    Appl ID . : ISR
6  Command       Enter TSO or Workstation commands     TSO logon : TWSPROC
7  Dialog Test   Perform dialog testing                TSO prefix: TSGMW
9  IBM Products  IBM program development products      System ID : RSMP
10 SCLM          SW Configuration Library Manager      MVS acct. : ACCT#
11 Workplace     ISPF Object/Action Workplace          Release . : ISPF 6.3
12 z/OS System   z/OS system programmer applications
13 z/OS User     z/OS user applications
M  More          Additional IBM Products
R  RSM           Additional RSM Products

     Enter X to Terminate using log/list defaults
```

Useful z/OS Commands

Useful z/OS Commands

- If you cannot issue them search the syslog via:
  - SDSF
  - eJES
  - Sysview
  - Etc…
- To see if they have been issued so you can collect the results

Some Useful Commands

```
D PROG,APF
D PROG,EXIT
D SMF,O
D SMS,OPTIONS
D IOS,CONFIG
D XCF,SYSPLEX
D CONSOLES
D IPLINFO (see next slide)
```

z/OS Command: D IPLINFO

- If you can issue commands the starting point should be:
  - D IPLINFO
  - Lists detail from the last IPL

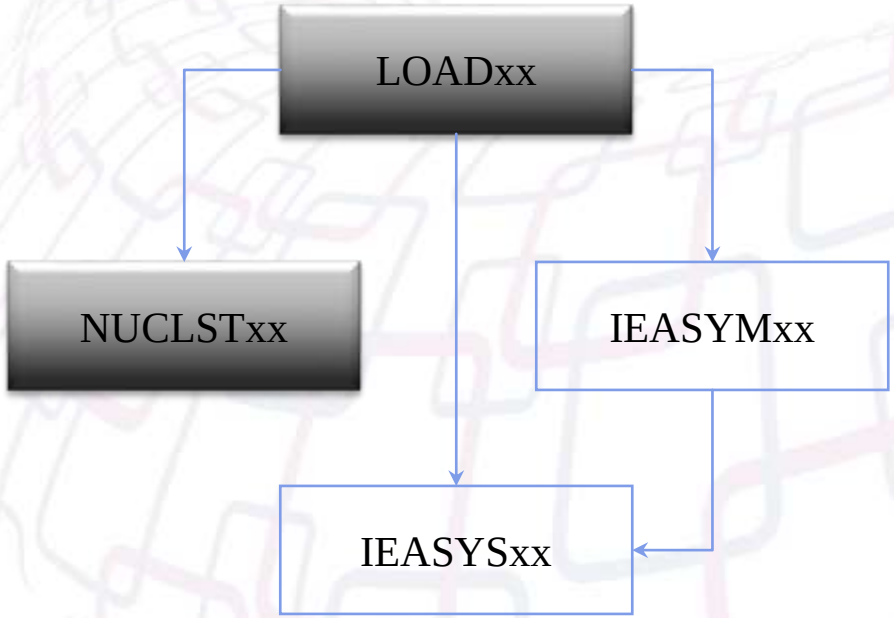
```
D IPLINFO
IEE254I  11.37.13 IPLINFO DISPLAY 870
SYSTEM IPLED AT 10.24.45 ON 11/07/2014
RELEASE z/OS 01.13.00    LICENSE = z/OS
USED LOADPB IN SYS2.IPLPARM ON 0082B
ARCHLVL = 2   MTLSHARE = N
IEASYM LIST = P0
IEASYS LIST = P0 (OP)
IODF DEVICE: ORIGINAL(0082B) CURRENT(0082B)
IPL DEVICE: ORIGINAL(00853) CURRENT(00853) VOLUME(PRES01)
```

LOADxx PARMLIB/IPLPARM Member

```
IODF      25 SYS2      ZOS1RSM
SYSCAT    PSYS01113CCATALOG.RSMP.MCAT.Z113
SYSPARM   P0
IEASYM    P0
NUCLST    00
PARMLIB   USER.PARMLIB
PARMLIB   ADCD.Z113H.PARMLIB
PARMLIB   SYS1.PARMLIB
NUCLEUS   1
SYSPLEX   LOCAL
INITSQA   0300K
```

System Configuration

- Specifies system image specific parameters.
- Root of all parameters
- Names the sysplex (optional, recommended) and the system image



- Defines the master catalog, nucleus, IEASYSxx member, IEASYMxx member (which can also specify (IEASYSxx), and parmlib concatenation.
- Has filters, enabling multiple system images to use same
- Should be in SYSn.IPLPARM
- Consider “,L” on SYSPARM statement
- Column dependent member
- Most values written to SYSLOG

Tools

To help you Footprint the system

IPLINFO

- Download and install IPLINFO Rexx Exec from Mark Zeldens website
  - http://www.mzelden.com/mvsutil.html
- No special privileges required, just reads information from Storage and creates a very useful output file
- But it's a long REXX exec; so you need to upload it to your system or sit and type it all in
- If you can upload this to one of your own datasets you can run the exec
- It simply reads in storage control blocks
- ……but returns a vast amount of useful information

IPLINFO – Basic Stuff

```
Today is Monday 2015-02-09 (2015.040). The local time is 11:33:38.

 The last IPL was Sunday 2015-02-08 (2015.039) at 02:24:35 (1 days ago).
 The IPL was done with CLPA.
 The system IPL address was 1234 (RES666).
 The IPL LOAD PARM used was RSM01.
 The local time offset from GMT time is -5 hours.
 The system is running in z/Architecture mode (ARCHLVL = 2).
 The Processor name is RSMES. The LPAR name is RSMP.
   RSMP is (HMC defined) LPAR ID = D and MIF ID = D.
   RSMP is PR/SM partition number 2 (internal value from the CSD).
 The sysplex name is RSMPLEX. This was system number 6 added to the sysplex.
 The GRS system id (SYSNAME) is RSMP. The SMF system id (SID) is RSMP.
 The currently active IODF data set is SYS4.IODFA1.
   Configuration ID = RSMP      EDT ID = 00
   TOKEN: Processor  Date      Time      Description
          VRSM2827B   14-06-24  13:49:42  SYS4    IODFA1
 The Master Catalog is CATALOG.MASTER.RSMP on CATRS6.
   The catalog alias level was 3 at IPL time.
     The catalog alias level is currently 3.
   The catalog type is ICF. SYS%-SYS1 conversion was not active at IPL time.
     SYS%-SYS1 conversion is not currently active.
```

IPLINFO – Good Stuff

```
LOADxx parameters from the IPA (LOADID):
    ARCHLVL   2
    IEASYM    (PL,L)
    IODF      ** SYS1      RSMP      00 Y
    NUCLEUS   1
    NUCLST    00
    PARMLIB   SYS1.RSMPLEX.ZOS
    PARMLIB   SYS1.PARMLIB
    PARMLIB   SYS1.OEM.PARMLIB
    SYSCAT    CATMV6133CCATALOG.MASTER.RSMP
    SYSPARM   (00,ID)
```

IPLINFO – Good Stuff

- But it also shows you:
  - All of the current libraries defined as:
    - APF Authorised
    - Linklisted
    - LPA
  - SMF Datasets
  - Dump Datasets
  - Page Datasets
  - All current subsystems

IPLINFO - ISPF

Look at the name of the EXEC… You call it whatever you like!!!

```
File  Edit  Transfer  Fonts  Options  Tools  View  Window  Help

  Menu  Utilities  Compilers  Hel

BROWSE    SYS2.SISPCLIB(IPL2) - 01.00                Line 00000000 Col 001 080
Command ===>                                                Scroll ===> PAGE
******************************** Top of Data ********************************
/* REXX */
/*                                          */
/* AUTHOR: Mark Zelden                      */
/*                                          */
/* Trace ?r */
/*****************************************************************************/
/*                                                                           */
/*   D I S C L A I M E R                                                     */
/*   -------------------                                                     */
/*                                                                           */
/* This program is FREEWARE. Use at your own risk.  Neither Mark             */
/* Zelden, nor other contributing organizations or individuals               */
/* accept any liability of any kind howsoever arising out of the use         */
/* of this program. You are free to use and modify this program as           */
/* you desire, however, the author does ask that you leave his name          */
/* in the source and give credit to him as the original programmer.          */
/*                                                                           */
/*****************************************************************************/
/* IPLINFO:  DISPLAY SYSTEM INFORMATION ON TERMINAL                          */
```

IPLINFO - ISPF

```
File  Edit  Transfer  Fonts  Options  Tools  View  Window  Help

BROWSE    Mark's MVS Utilities - IPLINFO                Line 00000000 Col 001 080
Command ===>                                                   Scroll ===> PAGE
********************************* Top of Data **********************************
*******************************************************************************
****************       IPLINFO - SYSTEM INFORMATION FOR VGID       ***************
*******************************************************************************

Today is Monday 2015-02-09 (2015.040). The local time is 10:38:36.

The last IPL was Sunday 2015-02-08 (2015.039) at 02:24:35 (1 days ago).
The IPL was done with CLPA.
The system IPL address was [redacted]
The IPL LOAD PARM used was [redacted]
The local time offset from GMT time is -5 hours.
The system is running in z/Architecture mode (ARCHLVL = 2).
The Processor name is [redacted]. The LPAR name is [redacted]
  [redacted] (HMC defined) LPAR ID = D and MIF ID = D.
  [redacted] PR/SM partition number 2 (internal value from the CSD).
The sysplex name is [redacted] This was system number 6 added to the sysplex.
The GRS system id (SYSNAME) is [redacted] The SMF system id (SID) is [redacted]
The currently active IODF data set is SYS4.IODFA1.
  Configuration ID = VGID      EDT ID = 00
  TOKEN: Processor  Date      Time      Description
         [redacted]  14-06-24  13:49:42  SYS4    IODFA1
```

ISPLINFO – In Batch

Remember I can call it whatever I like!!!

```
//HACK01  EXEC PGM=IKJEFT01,PARM=INFOLST
//SYSPROC  DD DISP=SHR,DSN=TSGMW.MY.REXXLIB
//SYSTSPRT DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSTSIN  DD DUMMY
//SYSIN    DD DUMMY
***JES2 msgs here ****
*************************************************************************
***************      IPLINFO - SYSTEM INFORMATION FOR RSMP      ***************
*************************************************************************

 Today is Monday 2015-02-09 (2015.040). The local time is 11:33:38.
```

TASID

- Is an IBM utility downloadable from here:
  - http://www-01.ibm.com/support/docview.wss?uid=swg24009131
- It's a more powerful ISPF based version of IPLINFO
- Some of the information will be exactly the same…
- But there are lots of good bits ☺

TASID – From the IBM Website

- The TASID system monitor allows you to view system activity on a z/OS system
- This includes information about active address spaces (batch jobs, started tasks, TSO users, and system tasks), ENQ activity and contention, initiator status on JES2 systems, and so on
- Note that there are some options that might not behave consistently or operate correctly on every level of z/OS.
- All available documentation is contained in the help panels, which you can access by pressing the HELP function key when on any panel within TASID

TASID – Screen Shots

TASID – Screen Shots

```
File  Navigate  Settings  View

-------- TASID: Active Subsystems                    LINE 00000001 COL 001 079
COMMAND ===> _                                              SCROLL ===> CSR
 ----------------------------+----------------------+-------------------------
 APF - APF Authorized libs   | PAR - LPAR info      | SPA - DASD space
 LIN - Linklst PRM - Parmlib | STG - Storage info   | SVC - SVC list
 LPA - LPA lib SYM - Symbols | NUC - Nucleus map    | UCB - Active devices
 LPD - Link Pack Directory   | SUB - Subsystems     | UNI - Available units
 ----------------------------+----------------------+-------------------------
                                   Subsystems


                         Printable names

AXR  CSQ7 DJAG JES2 MSTR QCBB QCBE RACF TNF  VAP
CICS DB9G IF01 JRLM OAM1 QCBC QCBF RRS  TWSC VMCF
CPB1 DFRM IRLM LOGR QCBA QCBD QCBI SMS  TWST

          Unprintable names (and their hex values)


  *ASIDBRO
```

```
MA   0.5 02/13/15.044 07:01AM 192.168.150.15   a   4,15
```

TASID

- This is an extremely powerful utility and as you can see from the previous screen there is lots to be displayed
- Option 8 of the Primary Menu is a Snapshot facility
- It writes the OP to a sequential dataset for browsing and saving….

TASID - Snapshot

```
Menu  Utilities  Compilers  Help

BROWSE    TSGMW.TASID.SNAPSHOT                          Line 00000000 Col 001 080
Command ===> _                                                 Scroll ===> CSR
********************************* Top of Data ***********************************
TASID Snapshot - TASID Version 5.21                      (201306211237)

Current time  12:11 on 2015/02/13       +-------------------------+
Last IPL time 10:24 on 2014/11/07       | TSO Users             9 |
                                        | Started Tasks        30 |
OS/390    01.13.00 JES Version  JES2    | Jobs                  4 |
SMF ID    RSMP     JES ........ z/OS1.13| System Addrs         32 |
User ID   TSGMW    RACF ....... 7.78.0  | Free Initiators       8 |
Nodename  RSMP     TSO ........ 3.13.0  |-------------------------|
Vtamaddr  A05TCP37 VTAM ....... 6.1     | Total                83 |
Procname  TWSPROC  DFP ........ 1.13.0  +-------------------------+
Region    2047M    DSS ........           CPU utilization    98%
RACF Grp  #RSM     DSF ........ 1.17.0    CPU 2818-M05      3 CPUs
Mode      PR/SM    ISPF ....... 6.3.0     Real Storage        314572K
LPARs              HSM ........ 01.13     ENQ Contention     None

Sysres: PRES01      System: RSMP        PLEX: LOCAL
IPL Load Parm: 082B PB M 1
   *ISRBROB

M^A                 0.1 02/13/15.044 07:13AM 192.168.150.15        a      4,15
```

SHOWMVS

- Is a CBT tape (www.cbttape.org) download that is extremely powerful
- There is a sample output file from a few years ago that shows you how powerful this utility is:
  - http://planetmvs.com/userexperiences/os390r8s.txt
- It can be found on the CBT downloads page:
  - http://www.cbttape.org/cbtdowns.htm

MXI

- Was originally developed as Shareware by a UK based techie called Rob Scott
- Rob then sold his idea and software to Rocket software
- However, there are still some of the original freeware versions out there and installed
- And the original is still available as a CBT Tape download

MXI - Screenshot

```
File  Dataset  Module  Unit  System  Plex  SMS  Storage  MQ  DB2  RACF  Tool

MXI - MENU - RSMP - HOME ----- CPU 100 UIC 2540 PAG    0 ---------- Row 1 of 85
Command ===> _                                              Scroll ===> PAGE

Command          Comment                          Group
AGRP             SMS Aggregate Groups             SMS
APF              APF List Datasets                DATASET
ASID             Address Space Usage Information  SYSTEM
CAT              Catalog Information              DATASET
CA1              CA-1 Configuration Information   SMS
CDE              JPAQ and TCB loaded modules      MODULE
CHP              Online Channel Paths             UNIT
CPF              Command Prefix Table             SYSTEM
CPU              CPU and LPAR Information         UNIT
CS               Common Storage Usage             STORAGE
CSR              Common Storage Remaining         STORAGE
DA               Active Address Space Information SYSTEM
DA ONLY(JOB)     Active Batch Jobs                SYSTEM
DA ONLY(STC)     Active Started Tasks             SYSTEM
DA ONLY(TSU)     Active TSO Users                 SYSTEM
DASD             Online DASD Information          UNIT
DASD NOT(SMS)    Online Non-SMS DASD Volumes      UNIT
  *DSLIST
```

MXI - Screenshot

```
  File  Dataset  Module  Unit  System  Plex  SMS  Storage  MQ  DB2  RACF  Tool

MXI - PARM - RSMP - HOME ----- CPU 100 UIC 2540 PAG    0 ---------- Row 1 of 62
Command ===> _                                              Scroll ===> PAGE

Dataset                                   Volume
USER.PARMLIB
ADCD.Z113H.PARMLIB
SYS1.PARMLIB

Statement                                                          Member
APG=7                                                              Default
CLOCK=00                                                           IEASYSP0
CMB=(UNITR,COMM,GRAPH,CHRDR)                                       IEASYSP0
CMD=P0                                                             IEASYSP0
CON=(P0,NOJES3)                                                    IEASYSP0
COUPLE=P0                                                          IEASYSP0
CSA=(3000,400000)                                                  IEASYSP0
CSCBLOC=ABOVE                                                      Default
DEVSUP=P0                                                          IEASYSP0
DIAG=P0                                                            IEASYSP0
DUMP=DASD                                                          IEASYSP0
FIX=P0                                                             IEASYSP0
  *DSLIST
```

ISRDDN

- Contained within ISPF is a debugging tool, ISRDDN, which can be used in TSO to:
  - Examine the datasets allocated to a DD name
  - Browse storage that is accessible to non-authorized callers
  - Identify the 'fetch location' for a module loaded by the user
  - Find the data sets which contained a specific member
  - Identify I/O errors caused by mixed record format allocations
  - Find who is allocated specific data sets
  - Identify member names or LPA load modules are duplicated in the user's
  - current allocations
  - Find empty datasets in data set concatenations

Getting into ISRDDN

- ISRDDN is invoked from any place in ISPF where you can enter a TSO command

```
  Menu  List  Mode  Functions  Utilities  Help
                                ISPF Command Shell
Enter TSO or Workstation commands below:

===> isrddn_

Place cursor on choice and press enter to Retrieve command

=>
=>
=>
=>
=>
=>
=>
=>
=>
=>

  *CMD
```

First ISRDDN Panel

- The first/home ISRDDN panel is a list of the DD names allocated to the TSO session and the data sets allocated to those DDNAMES

```
                          Current Data Set Allocations            Row 1 of 153
Command ===> _____________________________________________ Scroll ===> PAGE

 Volume   Disposition Act DDname   Data Set Name   Actions: B E V M F C I Q
 PDBA01   SHR,KEEP    > _ ADMCDATA QMFA10.ADMCDATA
 PDBA01   SHR,KEEP    > _ ADMCFORM QMFA10.SDSQCHRT
 PDBA01   SHR,KEEP    > _ ADMGGMAP QMFA10.SDSQMAPE
 PDBA01   SHR,KEEP    > _ ADMSYMBL QMFA10.ADMSYMBL
          MOD,DEL     > _ AOFPRINT ---------- JES2 Subsystem file -------------
 PRES01   SHR,KEEP    > _ AOFTABL  AUT330.AOFTABL
 PRES01   SHR,KEEP    > _ DITPLIB  DIT130.SDITPLIB
 PDBA01   SHR,KEEP    > _ DSNETBLS DSNA10.SDSNSPFT
          MOD,DEL     > _ DSQDEBUG ---------- JES2 Subsystem file -------------
 PWRK01   NEW,DEL     > _ DSQEDIT  SYS14231.T102034.RA000.TSGDL.R0162211
 PDBA01   SHR,KEEP    > _ DSQPNLE  QMFA10.DSQPNLE
          MOD,DEL     > _ DSQPRINT ---------- JES2 Subsystem file -------------
          MOD,DEL     > _ DSQUDUMP ---------- JES2 Subsystem file -------------
 PRES01   SHR,KEEP    > _ IHVCONF  AUT330.IHVCONF
 PWRK02   NEW,DEL     > _ ISPCTL1  SYS14231.T102034.RA000.TSGDL.R0162207
 PWRK02   NEW,DEL     > _ ISPCTL2  SYS14231.T102034.RA000.TSGDL.R0162208
 PRES01   SHR,KEEP    > _ ISPEXEC  ISP.SISPEXEC
 PRES01   SHR,KEEP    > _          SYS1.SBPXEXEC
 PSYS01   SHR,KEEP    > _          CSQ710.SCSQEXEC
  *CMD
```

ISRDDN Overview

- Commands Available
  - B Browse the first sixteen data sets or a single data set.
  - E Edit the first sixteen data sets or a single data set.
  - V View the first sixteen data sets or a single data set.
  - M Show an enhanced member list for the first sixteen data sets or a single data set
  - F Free the entire DDNAME.
  - C Compress a PDS using the existing allocation.
  - I Provide additional data set information.
  - Q Display list of users or jobs using data set.

Pseudo-DD names

- You can look at APF, PARMLIB, and LPA information with these commands:
  - APF: Include or remove a pseudo-ddname of APFLIST which contains a list of APF libraries.
  - LPA: Include or remove pseudo-ddnames LPALIB and LINKLIST which contain LPA libraries and Link List libraries respectively.
  - PARMLIB: Include or remove a psuedo-ddname of PARMLIB which contains a list of PARMLIB libraries.

Looking at a Load Module

- The LOAD command attempts to load a module into storage

```
                              Current Data Set Allocations              Row 1 of 153
Command ===> load iefbr14_                                          Scroll ===> PAGE

 Volume   Disposition Act DDname   Data Set Name   Actions: B E V M F C I Q
 PDBA01   SHR,KEEP    > _ ADMCDATA QMFA10.ADMCDATA
 PDBA01   SHR,KEEP    > _ ADMCFORM QMFA10.SDSQCHRT
 PDBA01   SHR,KEEP    > _ ADMGGMAP QMFA10.SDSQMAPE
 PDBA01   SHR,KEEP    > _ ADMSYMBL QMFA10.ADMSYMBL
          MOD,DEL     > _ AOFPRINT ---------- JES2 Subsystem file -------------
 PRES01   SHR,KEEP    > _ AOFTABL  AUT330.AOFTABL
 PRES01   SHR,KEEP    > _ DITPLIB  DIT130.SDITPLIB
 PDBA01   SHR,KEEP    > _ DSNETBLS DSNA10.SDSNSPFT
          MOD,DEL     > _ DSQDEBUG ---------- JES2 Subsystem file -------------
 PWRK01   NEW,DEL     > _ DSQEDIT  SYS14231.T102034.RA000.TSGDL.R0162211
 PDBA01   SHR,KEEP    > _ DSQPNLE  QMFA10.DSQPNLE
          MOD,DEL     > _ DSQPRINT ---------- JES2 Subsystem file -------------
          MOD,DEL     > _ DSQUDUMP ---------- JES2 Subsystem file -------------
 PRES01   SHR,KEEP    > _ IHVCONF  AUT330.IHVCONF
 PWRK02   NEW,DEL     > _ ISPCTL1  SYS14231.T102034.RA000.TSGDL.R0162207
 PWRK02   NEW,DEL     > _ ISPCTL2  SYS14231.T102034.RA000.TSGDL.R0162208
 PRES01   SHR,KEEP    > _ ISPEXEC  ISP.SISPEXEC
 PRES01   SHR,KEEP    > _          SYS1.SBPXEXEC
 PSYS01   SHR,KEEP    > _          CSQ710.SCSQEXEC
  *CMD
```

Looking at a Load Module…

- …if successful, ISRDDN shows the module statistics…

```
C                                                                    153
                          CSVQUERY Results                   IEFBR14  PAGE
  Command ===> _____________________________________________________
                                                   More:      +       Q
  Module IEFBR14  was found to be already loaded. Note that
  invocations of this program name may pick up another copy from
  STEPLIB or a LIBDEF'ed data set or from a tasklib such as ISPLLIB.
  Tab to a box and press enter to view the module in storage.
     +-------------------------+                                     -----
     | PLPA resident           |
     | Module address:00DF5000 |
     | Module size:   00000008 |
     | Reentrant               |                                     -----
     | Serially reusable       |
     | Not loadable only       |
     | Authorized library      |                                     -----
     | Not Authorized program  |                                     -----
     +-------------------------+

 *CMD
```

Looking at a Load Module…

- …and the “object code.”

```
BROWSE    IEFBR14 PLPA Start:00DF5000 Size:00000008  Line 00000000 Col 001 080
Command ===> _                                                Scroll ===> 2
******************************** Top of Data *********************************
      +0 (00DF5000)   1BFF07FE 00000000                  * ...Ú....          *
******************************* Bottom of Data ********************************

  *CMD
```

Looking at a Load Module…

- You can ask ISRDDN to “disassemble” the load module with the DISASM command

```
 BROWSE    IEFBR14 PLPA Start:00DF5000 Size:00000008  Line 00000000 Col 001 080
 Command ===> DISASM_                                   Scroll ===> 2
********************************* Top of Data *********************************
      +0 (00DF5000)   1BFF07FE 00000000                  * ...Ú....          *
******************************** Bottom of Data *******************************

   *CMD
```

Looking at a Load Module..

- You will be asked if you are authorized to do this…

```
 BROWSE    IEFBR14 PLPA Start:00DF5000 Size:00000008  Line 00000000 Col 001 080
 Command ===> DISASM                                        Scroll ===> 2
******************************** Top of Data *********************************
      +0 (00DF5000)   1BFF07FE 00000000                  * ...Ú....          *
******************************* Bottom of Data ********************************

                    *** WARNING ***
                    *** WARNING ***
                                                   More:   -
  Before using this function you must be aware of and
  respect the intellectual property rights of others.
  You are not authorized to use this function to
  disassemble, copy or create assembly listings
  or disassembled Assembler Language source code
  in violation of any contractual or other legal
  obligation. You are authorized to use this function
  only for code for which you have verified you have
  the right to perform disassembly.

  Only type YES to proceed if you believe you have the
  legal right to view the disassembled code.
    Type YES to proceed . . . NO
    Disassemble from offset . 00000000
   *CMD
```

Looking at a Load Module…

- You may have to scroll down to enter “YES”…

```
BROWSE    IEFBR14 PLPA Start:00DF5000 Size:00000008  Line 00000000 Col 001 080
Command ===> DISASM                                        Scroll ===> 2
******************************** Top of Data *********************************
      +0 (00DF5000)   1BFF07FE 00000000                  * ...Ú....          *
******************************** Bottom of Data ******************************

                    *** WARNING ***
                    *** WARNING ***
                                                   More:    -
  Before using this function you must be aware of and
  respect the intellectual property rights of others.
  You are not authorized to use this function to
  disassemble, copy or create assembly listings
  or disassembled Assembler Language source code
  in violation of any contractual or other legal
  obligation. You are authorized to use this function
  only for code for which you have verified you have
  the right to perform disassembly.

  Only type YES to proceed if you believe you have the
  legal right to view the disassembled code.
    Type YES to proceed . . . YES _
    Disassemble from offset . 00000000
*CMD
```

Looking at a Load Module…

- And if you say “YES”, your module is disassembled.

```
 BROWSE    IEFBR14 PLPA Start:00DF5000 Size:00000008  Line 00000000 Col 001 080
 Command ===> _                                                Scroll ===> 2
********************************* Top of Data *********************************
(00DF5000)       +0   1BFF           A0000000 SR      R15,R15
(00DF5002)       +2   07FE                    BR      R14
(00DF5004)       +4   0000 0000               DC    X'00000000'
******************************** Bottom of Data *******************************
*CMD
```

Browsing Storage

- ISRDDN allows you to browse storage within your address space
  - Storage must be accessible to a key 8, non-authorize, problem state program
  - Command syntax is similar to TSO TEST/TESTAUTH
  - Can list arrays using the ARRAY format instruction
  - Can chain together lists using the CHAIN command
  - Can format lists of pointers using the ARRAYP

- Some interesting storage locations:
  - CVT: 10.?
  - RCVT: 10.? +3EO?
  - List of General Resource Classes: 10.?+3e0?+BC

Footprinting: Summary

- So as you can see there are many ways to footprint a system
- But where do we go from here…..
- Well the first thing is to…..

Protect yourself..

As best as you can

How do you protect yourself

- If the tools are installed protect them with Dataset and Program Protection
- Restrict who can upload tools to the system:
  - IND$FILE
  - FTP
  - etc
- Restrict who can download data from the system:
  - IND$FILE
  - FTP
  - SMTP
  - etc

Summary

- We will not be able to fully stop the very determined hacker
- But, what we must do is make it as difficult for them to be able to understand your system
- Use the tools yourself to check you system and see what out there
- See if you can find any weaknesses by testing your own systems
- We need to be proactive when we are protecting these systems

Questions

Contact Details

Mark Wilson

RSM Partners

markw@rsmpartners.com