



# RSM PARTNERS

*World Class Mainframe Experts*

**Mainframe Penetration  
Testing 101  
Session Code AJ**

**Mark Wilson  
RSM Partners**

1

## Agenda

Introductions

Getting the language right


What tools are out there

Reconnaissance/Footprinting

One and One is not always two!

Getting to first base

Summary



2

# Introduction













**ALREADY CALM**  
I'm the  
**Technical Director**

3






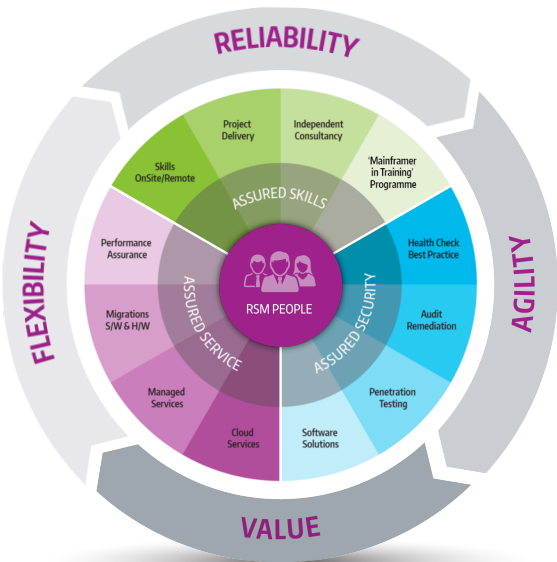
4





# About RSM



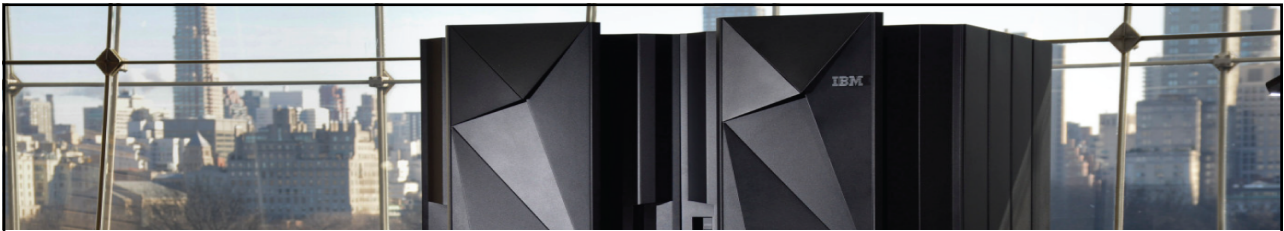
5



RSM Partners Mainframe Menu



6



## The IBM Mainframe!



7

## IBM Mainframe - Misconceptions

- The IBM mainframe is the most secure computing platform available to corporations today
  - Wrong - It is the most securable
- The IBM mainframe is unhackable
  - Wrong – Numerous successful hacks



8

## Married bank worker stole £2m then spent the lot on call girls: £1m went on ONE Thai escort

- John Skermer set up fake bank accounts with overdrafts of £1m
- The 45-year-old then siphoned cash into his personal account
- The computer geek spent months wining and dining a escort girl
- All the while Skermer's wife was in the dark about his infidelity

A married bank worker who stole more than £2million from Barclays and squandered it on prostitutes has been jailed for seven years.

John Skermer, 45, set up fake bank accounts with overdrafts of £1million, then siphoned the money into his personal account.

He spent almost all the cash on call girls, lavishing £1million on one escort alone. The computer geek spent months wining and dining the Thai woman, known as Kookai, travelling to London from his Cheshire home and taking her to expensive hotels and restaurants.



**RSM**  
PARTNERS  
MAINFRAME

9

NEWS

## Pirate Bay co-founder charged with hacking IBM mainframes, stealing money



Pirate Bay co-founder Gottfrid Svartholm Warg was charged with hacking the IBM mainframe of Logica, a Swedish IT firm that provided tax services to the Swedish government, and the IBM mainframe of the Swedish Nordea bank, the Swedish public prosecutor said on Tuesday.

"This is the biggest investigation into data intrusion ever performed in Sweden," said public prosecutor Henrik Olin.



Gottfrid Svartholm Warg

IDGNS

Besides Svartholm Warg, the prosecution charged three other Swedish citizens.

[ Further reading: [The best media streaming devices](#) ]

Two of them live in Malmö and provided accounts for money transfers while one other—who lives in the middle of Sweden—

was charged with mainframe hacking, Olin said.

**RSM**  
PARTNERS  
MAINFRAME

10

## IBM Mainframe - Misconceptions

The Mainframe is Dead!

I announced the death of the mainframe, it's time to put the poor thing out of its misery. I declare the mainframe finally.... DEAD..... RIP

InfoWorld editor Stewart Alsop in 1991

*"I predict that the last mainframe will be unplugged on March 15, 1996"*

*That should have happened many many years ago!!*



11

LOOKING FOR something truly **POWERFUL?**



# 1.2

MILLION

*Transactions per second*

IBM **CICS & z Systems**

By the year 2020 there will be over **30 bn** connected devices



**CICS is ready**

RESTful JSON interface  
Mobile Workload Pricing  
Powerful, reliable, scalable

**1 IBM z13**



with **CICS V5.3** can produce this **amazing** throughput

**The platform of choice**

**36% faster** mobile response times

Can handle **100x the workload** of Cyber Monday



12




**MAINFRAMES  
RUN THE WORLD!**

- 71% of Fortune 500 companies use mainframes
- 92 of the world's top 100 banks use mainframes
- 23 of the world's top 25 retailers use mainframes
- All of the world's top 10 insurers use mainframes
- They handle 90% of all credit card transactions
- They hold 70% of the world's business data

**ANY QUESTIONS?**

**RSM  
PARTNERS**  
Z MAINFRAME

13



**Getting the language right**

**RSM  
PARTNERS**  
Z MAINFRAME

14

## Getting the language right

### Security Assessment

- Reviewing the security settings of a site to identify any security weaknesses.
- Requires high level of authority



15

## Getting the language right

### Vulnerability Scanning

- Scanning the code delivered by IBM and ISV's along with any code you may have developed yourself
- Test the code to see if it has any vulnerabilities that could be exploited by a knowledgeable user

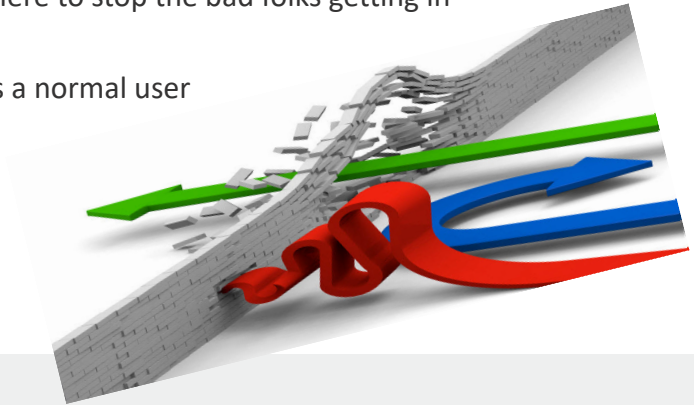


16

## Getting the language right

### Penetration Testing

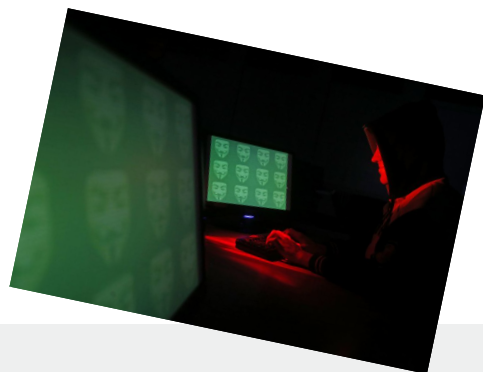
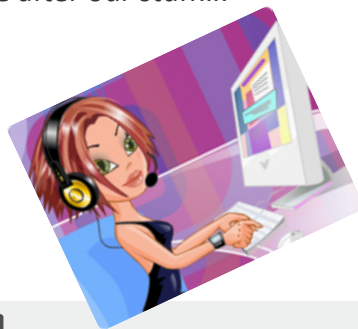
- Done by the good people out there to stop the bad folks getting in
- This is the bit I enjoy the most
- Should have the same access as a normal user



## Getting the language right

### Hacking

- The bad guys or gals..... its not necessarily a male dominated activity these days
- They are after our stuff....



## What we will be focusing on

- What is Penetration Testing?
- Wikipedia Definition:
- “A penetration test is a method of evaluating the security of a computer system or network by simulating an attack by a malicious cracker.”
- What is it...
  - A security test with permission
  - Uses techniques employed by the bad guys
  - Designed not to disrupt your system
  - Identify security issues to minimise the risk of an attacker compromising your system
  - Basically we try to find holes in your system before somebody else does!



19

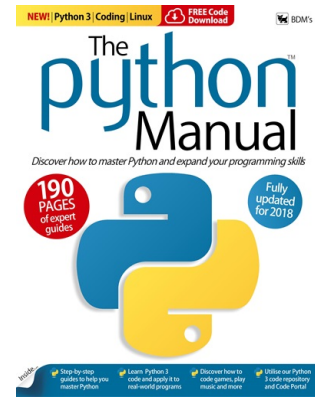
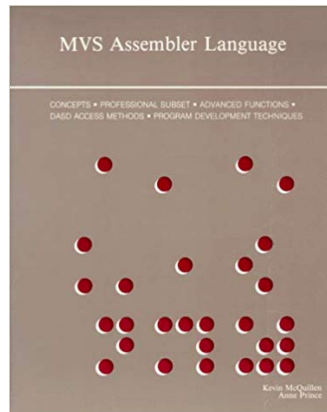
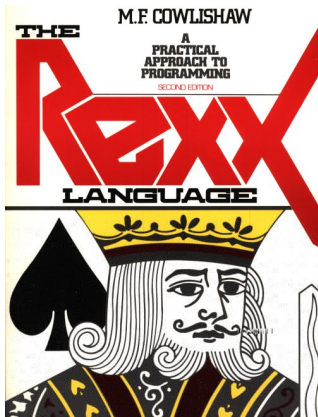


## Skills Needed?



20

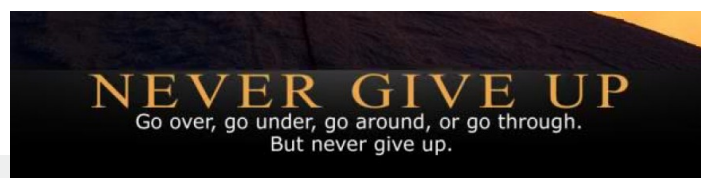
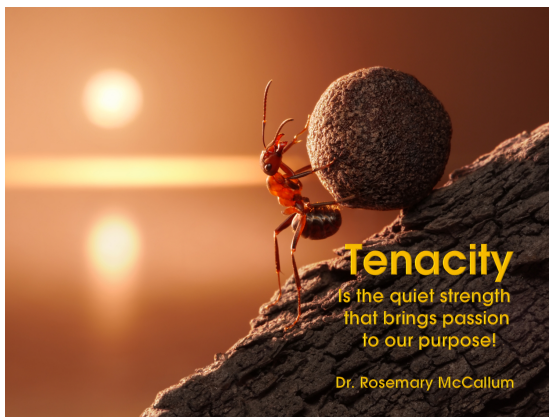
## Skills needed?



**RSM**  
**PARTNERS**  
**MAINFRAME**

21

## Personality Traits!!



**RSM**  
**PARTNERS**  
**MAINFRAME**

22



## Integrity



23

23

## z/OS System Integrity: IBM's Definition

- First issued in 1973, IBM's MVS System Integrity Statement, and subsequent statements for OS/390 and z/OS, has stood for over three decades as a symbol of IBM's confidence in and commitment to the z/OS operating system
- IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security – that is, to prevent them from gaining access, circumventing, disabling, altering, or obtaining control of key z/OS system processes and resources unless allowed by the installation



24

## z/OS System Integrity: IBM's Definition

- Specifically, z/OS "System Integrity" is defined as the inability of any program not authorized by a mechanism under the installation's control to circumvent or disable store or fetch protection, access a resource protected by the z/OS Security Server (RACF), or obtain control in an authorized state; that is, in supervisor state, with a protection key less than eight (8), or Authorized Program Facility (APF) authorized
- The Authorized Program Facility (APF) is the primary mechanism provided for this purpose. It allows authorization of system-level programs that need to modify or extend the basic functions of the operating system



25



## APF Authorization in Action - Rules of the Road



26

26



The system runs in “problem state”. Meaning the set of privileged instructions is not available. Only when the “problem program” is in “supervisor state” can these privileged instructions be used. APF authorization of programs, however granted, permits their use.

APF Datasets are defined to the system at a very early stage of the IPL process. As a result the system has no knowledge of their actual existence and loads “as is”. Errors in naming lead to Post-IPL APF vulnerabilities if they are allocated.	LNKST Datasets are APF Authorized by default. Or not, when the value of the IEASYS Parameter LNKAUTH is set to APFTAB. Only those Modules in either APF/LNKST marked by the author as AC1 will actually be granted APF authorized access.	If a library is in the LNKST concatenation but is not APF-authorized, the system will consider the library to be unauthorized for the duration of the job or step if the library is referred to through a JOBLIB or STEPLIB DD statement.	It is not necessary for the datasets in the LPALST to be APF-authorized. However, any module in the link pack area (pageable, modified, fixed, or dynamic LPA) is treated by the system as though it came from an APF authorized library.	PSW keys 0 - 7 are used by the z/OS base control program (BCP) and various subsystems and middleware. Key 0 is the master key. PSW keys 8 through 15 are assigned to users. The Program Properties Table can be used to modify expected PSW key values.
--	---	---	---	---

Properly protect LNK and LPA data set to avoid system security and integrity exposures, just as you would any APF-authorized library

27



## What's an ESM and what do they do?

28

## What is an ESM and what do they do?

- ESM = External Security Manager
- There are three of them today:
  - IBM® RACF® (RACF) \*Also version for z/VM
  - CA ACF2™ (ACF2) \* Also version for z/VM
  - CA Top Secret® (TSS) \* Also version for z/VM and z/VSE
- They have many roles to perform:
  - Authentication (Users)
  - Authorization (Data and Users)
  - Logging (Data and Users)



29

## Authentication

- Service provided by all three ESM's
  - Traditional User Name and Password (8 characters)
  - Passphrases (9-100 characters)
  - Passtickets (digital certificates)
  - Multi Factor Authentication (MFA) or Advanced Authentication



30

## Authorization

- A function provided by the ESM's to check if something has access to something
- However the ESM doesn't actually check access!
- The resource manager asks the ESM a question
  - Can Carla access SYS1.IPLPARM, with UPDATE?
  - The ESM responds with a YES, NO or Don't Know!
- The resource manager then decides how to process the response
- The normal response is that the resource manager ALWAYS does what the ESM says.... well sort of!!



31



## What non mainframe tools are out there today?



32

## What tools are out there today?

- Do a simple google search
  - mainframe pentesting tools or mainframe hacking tools
- There is plenty to read and research



33

## What

A screenshot of a Google search results page for the query 'mainframe hacking tools'. The search bar at the top shows the query and a magnifying glass icon. Below the search bar, there are tabs for 'All', 'Images', 'News', 'Videos', 'Shopping', 'More', 'Settings', and 'Tools'. The search results show 'About 997,000 results (0.35 seconds)'. The first result is 'Pwning the mainframe: How to hack the "most secure" platform on ...' with a link to 'https://www.zdnet.com/article/hacking-mainframe-black-hat-talk-secure-platform/'. The second result is 'How to Make Your Mainframe Hard to Hack | Mainframe Cybersecurity' with a link to 'https://compuware.com/make-your-mainframe-hard-to-hack/'. The third result is 'Evil Mainframe Training' with a link to 'https://evilmainframe.com/'. The fourth result is '2017 - A New Look at Mainframe Hacking and Penetration Testing v2.2' with a link to 'https://www.slideshare.net/.../2017-a-new-look-at-mainframe-hacking-and-penetration...'. The fifth result is 'SHARE : Blogs : Young, the Mainframe Hacker: Tools and Rules' with a link to 'https://www.share.org/blog/young-the-mainframe-hacker-tools-and-rules'. The sixth result is 'Black Hat Europe 2018 | Evil Mainframe Hacking' with a link to 'blackhat.com/eu-18/training/evil-mainframe-hacking.html'. The search results are displayed in a list format with blue links and green text for the first result. The RSM PARTNERS MAINFRAME logo is visible in the bottom left corner of the slide.

34

Popular repositories

**Mainframed**  
Mainframe security auditing and scripts  
● Shell ★ 78 🍴 17

**MFSniffer**  
Mainframe TN3270 unencrypted TSO session user ID and password sniffer  
● Python ★ 36 🍴 8

**logica**  
Files compiled from the Logica breach investigation materials  
● C ★ 31 🍴 7

**nmapdb**  
Forked from [argp/nmapdb](#)  
Parse nmap's XML output files and insert them into an SQLite database  
● Python ★ 25 🍴 3

**Enumeration**  
PoC REXX Script to Help with z/OS System enumeration via OMVS/TSO/JCL.  
★ 24 🍴 7

**MainTP**  
Mainframe Transfer: PROTOCOL  
● Python ★ 19 🍴 9

35

## CICSPWN - <https://github.com/ayoul3/cicspwn>

ayoul3 / cicspwn

Watch 4 Star 43 Fork 15

Code Issues 3 Pull requests 1 Projects 0 Wiki Security Insights

CICSpwn is a tool to pentest a CICS Transaction servers on z/OS.

82 commits 2 branches 0 releases 2 contributors

Branch: master New pull request Find File Clone or download

ayoul3 Add files via upload Latest commit a883799 on 12 Feb 2017

README.MD	Update README.MD	3 years ago
cicspwn.py	Add files via upload	2 years ago
ftp_cmds.txt	Add files via upload	3 years ago

README.MD

### CICSpwn

#### Description

CICSpwn is a tool to pentest CICS Transaction servers on z/OS.

#### Features

- Get general information about CICS and the underlying z/OS
  - List available IBM supplied transactions
  - Get active sessions and userids
  - Get path (HLQ) of files and libraries

36

And don't forget.....

HERCULES

## The Hercules System/370, ESA/390, and z/Architecture Emulator

**Hercules** is an open source software implementation of the mainframe System/370 and ESA/390 architectures, in addition to the new 64-bit z/Architecture. Hercules runs under Linux, Windows (98, NT, 2000, and XP), Solaris, FreeBSD, and Mac OS X (10.3 and later).

Hercules is [OSI Certified Open Source Software](#) licensed under the terms of the [Q Public Licence](#).

Hercules was created by [Roger Fowler](#) and is maintained by Jay Maynard. Jan Jaeger designed and implemented many of the advanced features of Hercules, including dynamic reconfiguration, integrated console, interpretive execution and z/Architecture support. A dedicated crew of programmers is constantly at work implementing new features and fixing bugs.



**RSM**  
PARTNERS  
MAINFRAME

37

Uploads ▾ PLAY ALL SORT BY

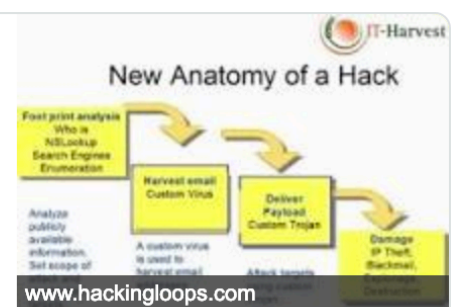
<p><b>Multitasking programming with IBM PL/I F compiler -</b> 147 views • 4 days ago</p>	<p><b>REXX Systems Programming - M62</b> 179 views • 1 week ago</p>	<p><b>An MVS 3.8 TK4 instance in the cloud for the moshix</b> 372 views • 1 month ago</p>	<p><b>Running Linux on a real IBM z13 mainframe with</b> 360 views • 1 month ago</p>	<p><b>Writing interactive Unix style utilities for TSO on MVS -</b> 316 views • 1 month ago</p>
<p><b>Systems Programming for z/OS or MVS - Writing TSO</b> 376 views • 1 month ago</p>	<p><b>z/OS systems programming - obtaining OS data from the</b> 367 views • 1 month ago</p>	<p><b>An archaeological expedition back in time to IBM OS/360 -</b> 410 views • 1 month ago</p>	<p><b>Operate your MVS console remotely with IMON - M55</b> 223 views • 1 month ago</p>	<p><b>Do you own an old mainframe printout? - M54</b> 237 views • 2 months ago</p>
<p>1:08:51</p>	<p>30:48</p>	<p>19:03</p>	<p>32:48</p>	<p>29:54</p>

38



## Reconnaissance/Footprinting

**Footprinting** (also known as reconnaissance) is the technique used for gathering information about computer systems and the entities they belong to. To get this information, a **hacker** might use various tools and technologies. This information is very useful to a **hacker** who is trying to crack a whole system.



## Mainframe Specific+

- System Tools
  - D IPLINFO & IPLINFO
  - SHOWMVS
  - TASID
  - SYSLOG (SDSF, IOF, SYSVIEW, etc)
  - z/OS and JES Commands
  - Write your own
- List Servers
  - IBMMAIN
  - RACF-L
- Social Media (FB, Linkedin, Twitter etc)



41

## Some zOS Commands

System Service	Display	Modify	Set
APF Library list	D PROG,APF		T PROG=(xx)
LPA Library List	D PROG,LPA		
Linklist Library List	D PROG,LNKLST		
APPC (Advanced Pgm to Pgm Commun)	D APPC		T APPC=(xx,L)
ASCH (APPC scheduling)	D ASCH		T ASCH=(xx,L)
Consoles	D CONSOLES		
Console Groups (alternate console defn)	D CNGRP		T CNGRP=(xx,L)
Data Lookaside Facility (HIPERBATCH)		F DLF,STATUS	
I/O Subsystem configuration	D IOS,CONFIG		
MVS Messaging Service	D MMS		
Message Processing Facility	D MPF		
zOS PARMLIB	D PARMLIB		
System Management Facility	D SMF[,S][,O]		
Cross System Coupling Facility	D XCF,SYSPLEX	D XCF,COUPLE	D XCF,PRMPPOLICY
Storage Management Subsystem	D SMS[,A],[OPTIONS]		



42

## Other Ways to find information

- ISRDDN
  - Part of standard TSO
  - TSO ISRDDN
    - APF
      - Shows list of all currently APF Authorised Datasets
- MXI
  - You can still get a free version of this commercial product; very useful
- TASID
  - [http://www-01.ibm.com/support/docview.wss?rs=17&context=SSBLID&dc=D400&uid=swg24009131&loc=en\\_US&cs=UTF-8&lang=en](http://www-01.ibm.com/support/docview.wss?rs=17&context=SSBLID&dc=D400&uid=swg24009131&loc=en_US&cs=UTF-8&lang=en)
- SHOWzOS
  - <http://www.cbttape.org/>
- Something the sysprogs have written themselves!



43

## Other Ways to find information

- SYSLOG
  - Use your site's tool SDSF, EJES, etc
  - Browse the log; Look for ICH408I messages
  - You will find resource names, Userids and in some cases the password of a Userid
    - Ever typed in your password instead of your Userid!



44

## IPLINFO

- If you can issue commands the starting point should be:

- D IPLINFO
- Lists detail from the last IPL

RESPONSE=RSMP

```
IEE254I 18.26.07 IPLINFO DISPLAY 487
SYSTEM IPLED AT 12.49.51 ON 12/27/2018
RELEASE z/OS 02.03.00 LICENSE = z/OS
USED LOAD23 IN SYS2.IPLPARM ON 01000
ARCHLVL = 2 MTLSHARE = N
IEASYM LIST = (00,L)
IEASYS LIST = (00) (OP)
IODF DEVICE: ORIGINAL(01000) CURRENT(01000)
IPL DEVICE: ORIGINAL(01269)
CURRENT(01269) VOLUME(TSRB1A)
```



45

## Load Member

```
BROWSE    SYS2.IPLPARM(LOAD23) - 01.12          Line 0000000085 Col 001 080
Command ==>                                     Scroll ==> CSR
```

\*\*\*\*\*

\* LOCAL DEFINITIONS FOR RSMP

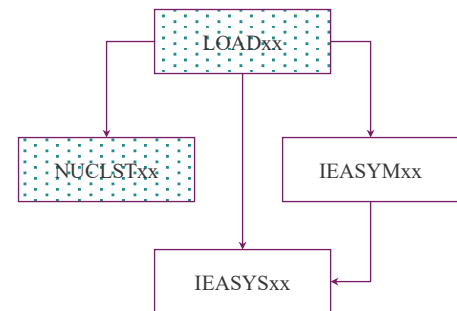
\*\*\*\*\*

```
LPARNAME RSMP
SYSPLEX TESTPLEX
IODF 38 SYS2 ZOS
SYSCAT PSYS11113CCATALOG.RSMP.MCAT.Z21 CATALOG
IEASYM (00,L)
SYSPARM (00,L)
PARMLIB SYS1.PARMLIB.TESTPLEX.Z23 TSYS01
PARMLIB SYS1.PARMLIB
PARMLIB SYS1.IBM.PARMLIB
*
```

46

## System Configuration

- Specifies system specific parameters.
- Root of all parameters
- 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



## IEASYSxx

```

BROWSE  SYS1.PARMLIB.TESTPLEX.Z23(IEASYS00) - 01 Line 0000000000 Col 001 080
Command ==> | Scroll ==> CSR
***** Top of Data *****
CLPA, DO A CLPA JUST TO BE SAFE.....
CLOCK=00, SELECT 00 FOR GMT, 01 FOR DST
CMB=(UNITR,COMM,GRAPH,CHDR), ADDITIONAL CMB ENTRIES
CMD=&SYSCONE.,
CON=(00,NOJES3), SELECT CONSOL00
COUPLE=00, RRS
CSA=(3000,400000), CSA RANGE
DEVSUP=00,
DIAG=00, SELECT DIAG00, DIAGNOSTIC COMMANDS
DUMP=DASD, PLACE SVC DUMPS ON DASD DEVICES
FIX=00, SELECT IEAFIX00, FIX MODULES SPECIFIED
GRS=STAR,
GRSRNL=00,
GRSCNF=00,
ILMMODE=NONE, EXPLICITLY DISABLE LICENSE MANAGER
IKJTSO=&SYSCONE., USE IKJTSOP0 FROM USER PARMLIB
LNKAUTH=LNKLST, AUTHORIZE LNKLST00, APFTAB IS ALTERNATE
LOGCLS=L, WILL NOT BE PRINTED BY DEFAULT
LOGLMT=999999, MAX WTL MESSAGES QUEUED, MUST BE 6 DIGITS
LOGREC=LOGSTREAM,
LPA=(00,&SYSCONE.,L), SELECT LPALST00
  
```

You know have.....



**RSM**  
**PARTNERS**  
**MAINFRAME**

49

## RACF Specific

- RACF SEARCH Command
  - WARNING (Dataset & General Resources)
  - SR NOMASK WARNING
  - SR CLASS(xxxxx) WARNING
- RACF LD Command
  - List all of the APF Authorised datasets
  - What access do you have?

**RSM**  
**PARTNERS**  
**MAINFRAME**

50

## Hints and Tips....

Do this as quietly as you can

## Screenshots

NotePad,  
save as TXT  
files

Collect all  
that you see,  
it may be  
important  
later!



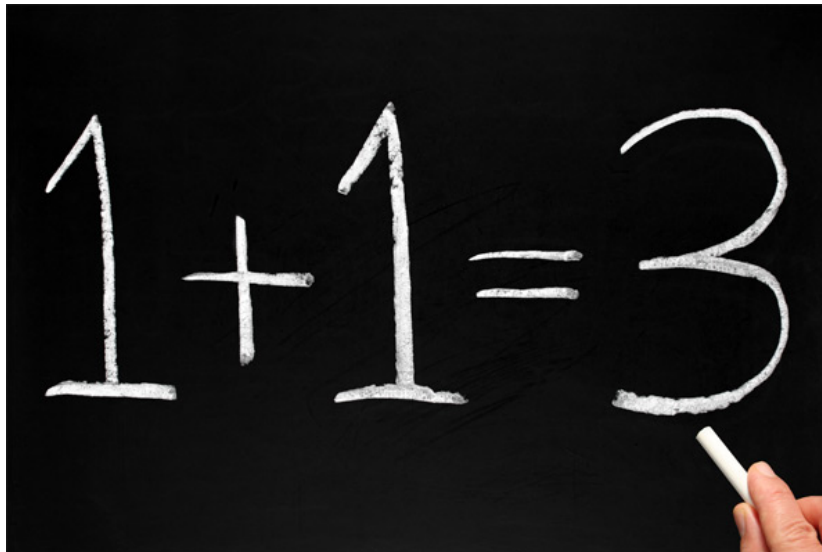
51



# One and One is not always two!

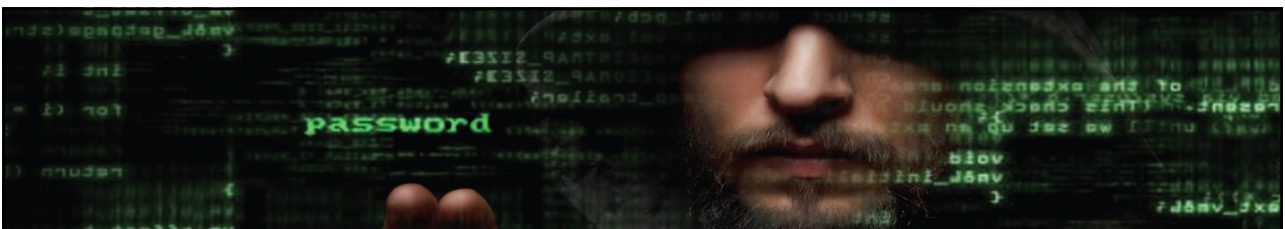


52



**RSM**  
PARTNERS  
MAINFRAME

53



## Getting to first base

**RSM**  
PARTNERS  
MAINFRAME

54

## Getting to first base

List the ESM  
system settings

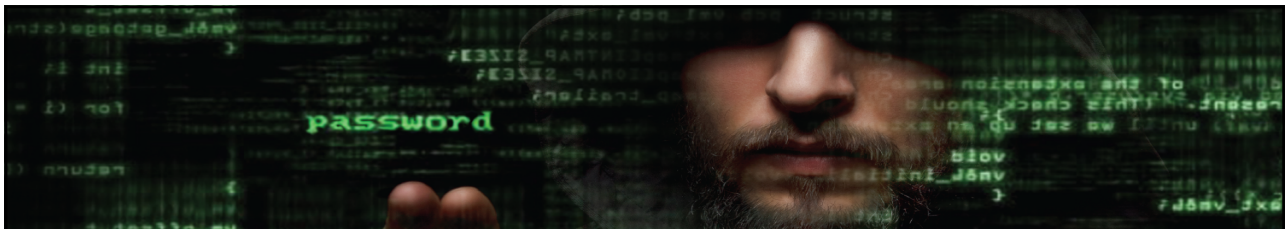
- RACF SETROPTS
- ACF2 GSO Options
- TSS TSSPRMxx

List all of the ESM  
profiles you have  
access to

List all of the APF,  
Linklist, Parmlib  
and Proclib  
datasets, do you  
have access?



55

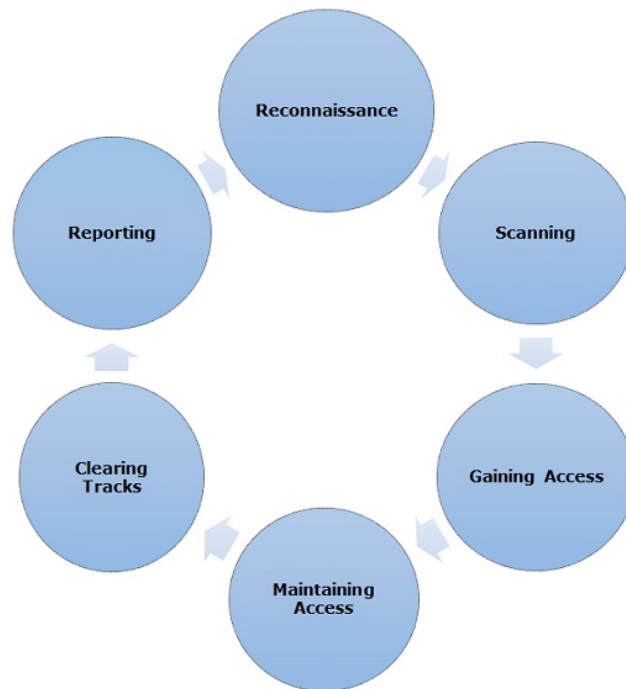


## Summary



56

## The Process



57

## Summary



Be patient!



Do it quietly, its more fun that way



Don't change anything on a running Production system!



If you can get access to a test system, use it!



Practice, Practice and Practice!!!!

58

## Thank you!

- Please complete the Session Evaluation!
- Session Code AJ
- Do it in the APP!!



© Copyright IBM Corporation 2019

59

A photograph of a two-story brick building with large windows. The building has the 'RSM PARTNERS' logo on the upper left side and a large 'Z' logo on the right side. The image is overlaid with a semi-transparent purple filter.

Mark Wilson  
Technical Director,  
RSM Partners

markw@rsmpartners.com  
office: +44 (0) 1527 837767  
mobile: +44 (0) 7768 617006

www.rsmpartners.com

**RSM PARTNERS Z MAINFRAME**

**US:**  
Suite 1600  
222 So. 9th Street  
Minneapolis MN 55402  
US  
T: +1 (612) 547-0089  
E: info@rsmpartners.com  
www.rsmpartners.com

**UK:**  
RSM House  
Isidore Rd  
Bromsgrove Enterprise Park  
Bromsgrove  
B60 3FQ  
UK  
T: +44 (0)1527 837767  
E: info@rsmpartners.com  
www.rsmpartners.com

60