z/OS VULNERABILITY SCANNING AND MANAGEMENT

Key Resources, Inc.
ray.overby@kr-inc.com
(312) KRI-0007
www.kr-inc.com

key resources, inc.
Ensuring System Integrity For z/Series

Ray Overby

- SKK - ACF2 Developer (1981-1988)
- Key Resources, Inc. incorporated in 1988
  - Systems Programming
  - Security Audit and Reviews
  - Security Product Development
- Developed ESM Conversion and Merge products
- Consulting & Development for RACF add-on ISV
- Common Criteria Lab doing vulnerability analysis
- Developed Automated Penetration Testing product
- z/OS Internals & Security expert

key resources, inc.

Ensuring System Integrity For z/Series

Agenda

- Demonstration of Integrity Based Exploit
- Discuss System Configuration Vulnerabilities
- Discuss External Security Manager (ESM) Vulnerabilities
- Discuss Integrity Vulnerabilities
- Summary

Demonstration - Exploit Setup

- TSO user logged in to TSO on a z/OS 1.13 system
- TSO user has no extraordinary security authority
- Requires the ability to create and execute a program
- Program does not require APF authorization

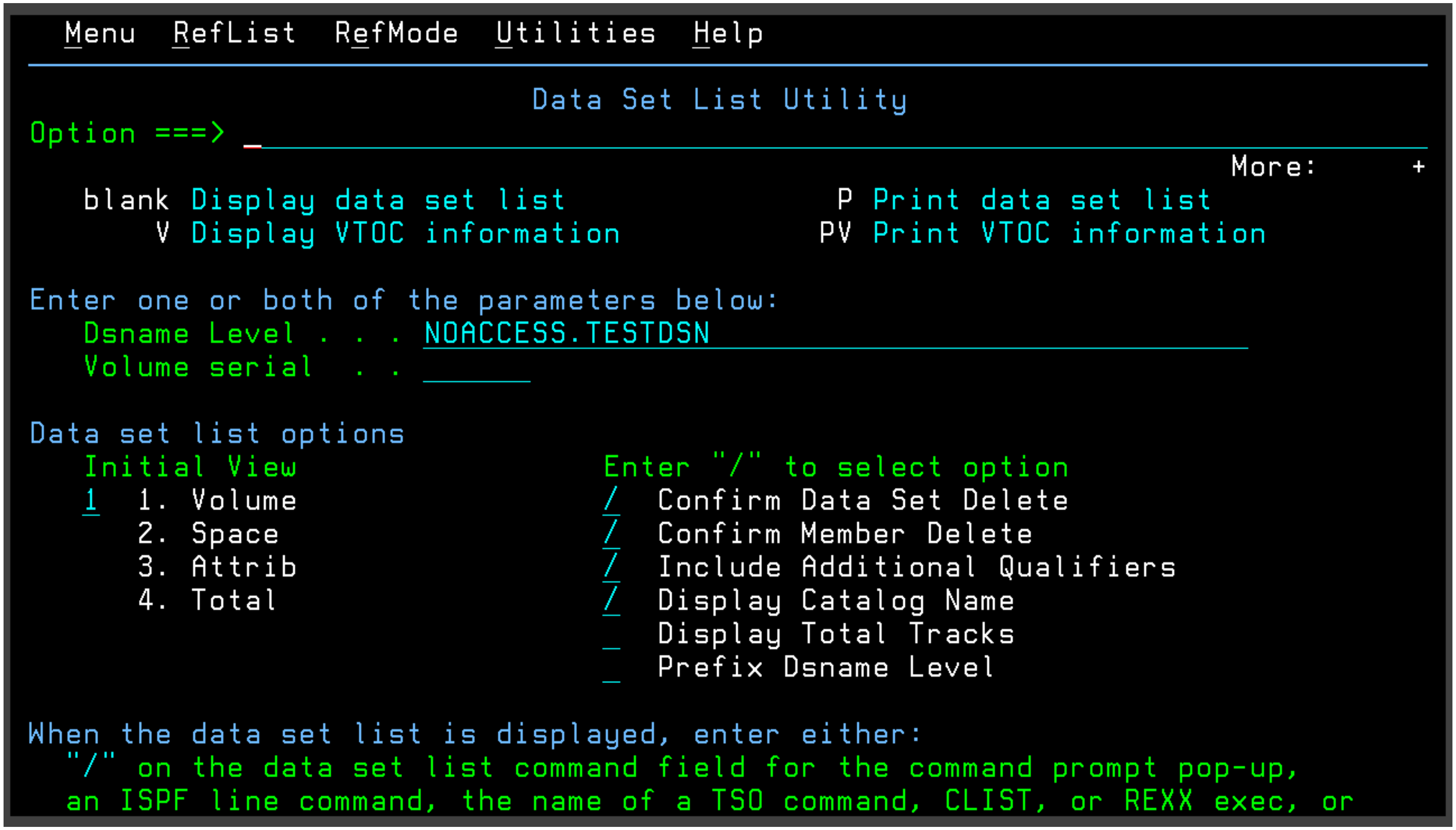
Demonstration Outline

- Demonstrate user does not have access to a dataset
- Execute the exploit program
- Demonstrate user now has access to the dataset (no RACF logging will occur)
- Note: External Security Manager (ESM) IBM-RACF. Exploit works with CA-ACF2 or CA-TSS with minor modifications.

Demonstration - Create the Exploit

- KRI will not share the Program details
- Type in the Program, Assemble and link edit
  - 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 …………..

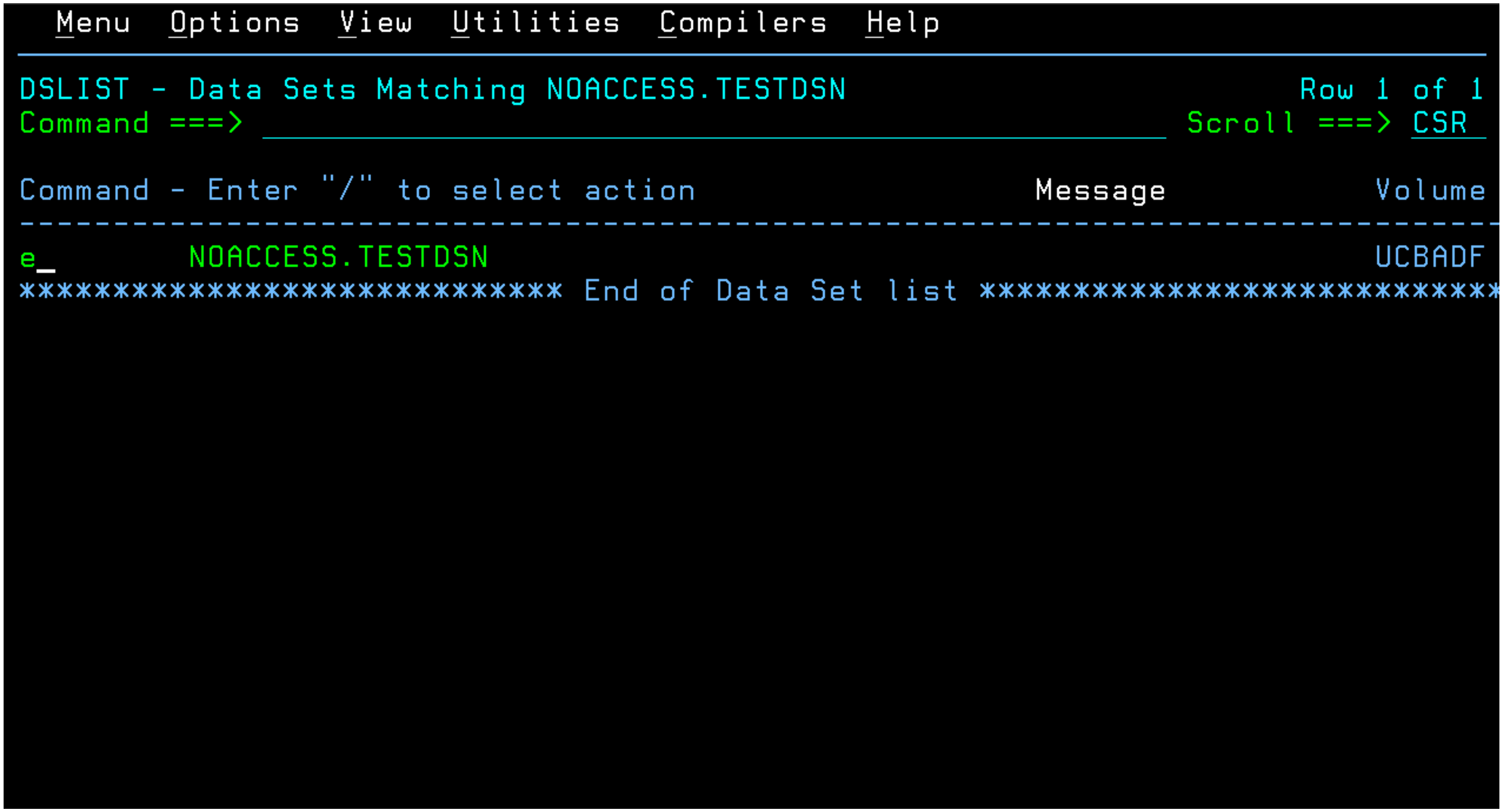
Demonstration - Access the Dataset –ISPF 3.4



```
  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
```

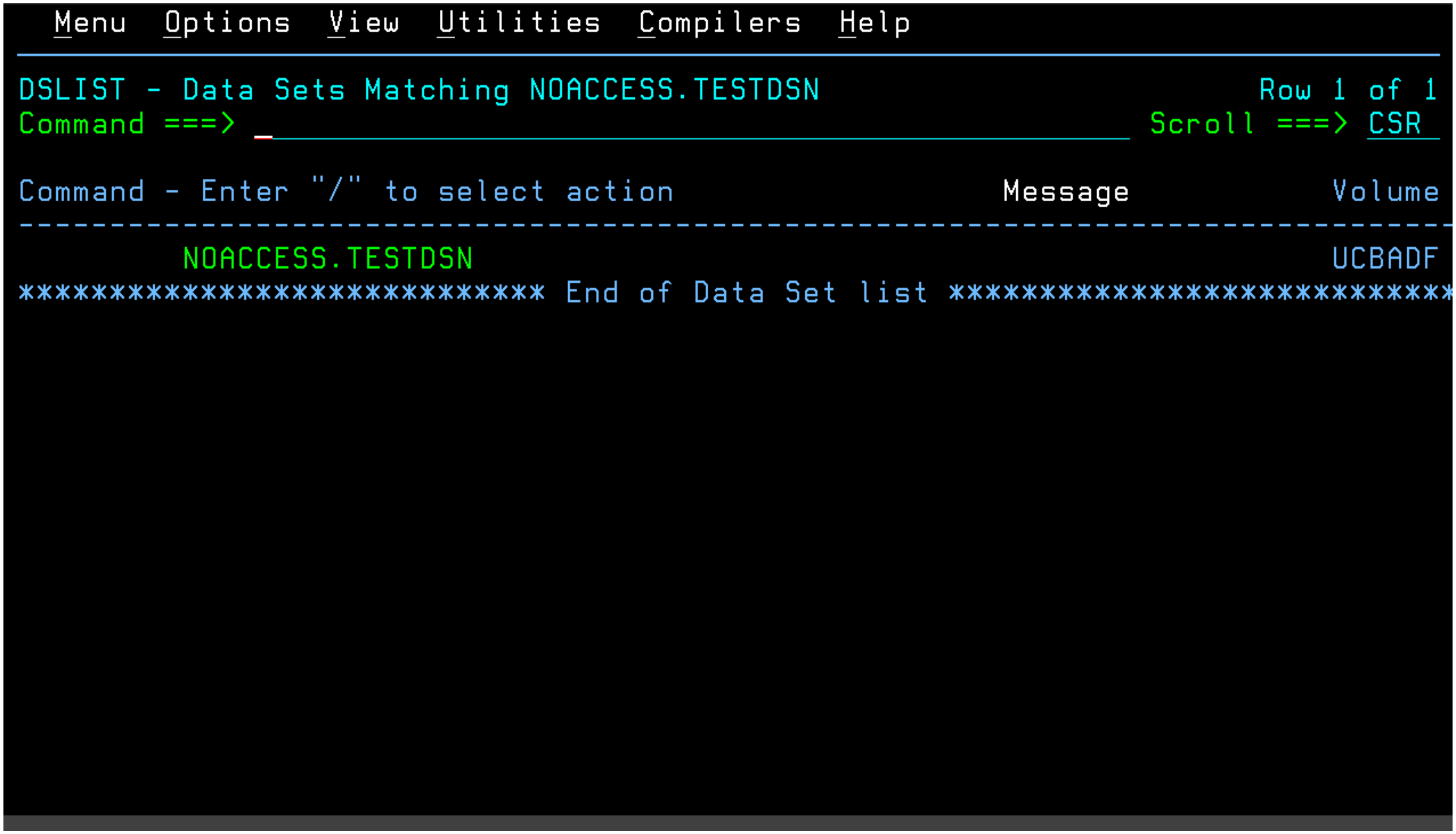
key resources, inc.
Ensuring System Integrity For z/Series

Demonstration - Edit the File



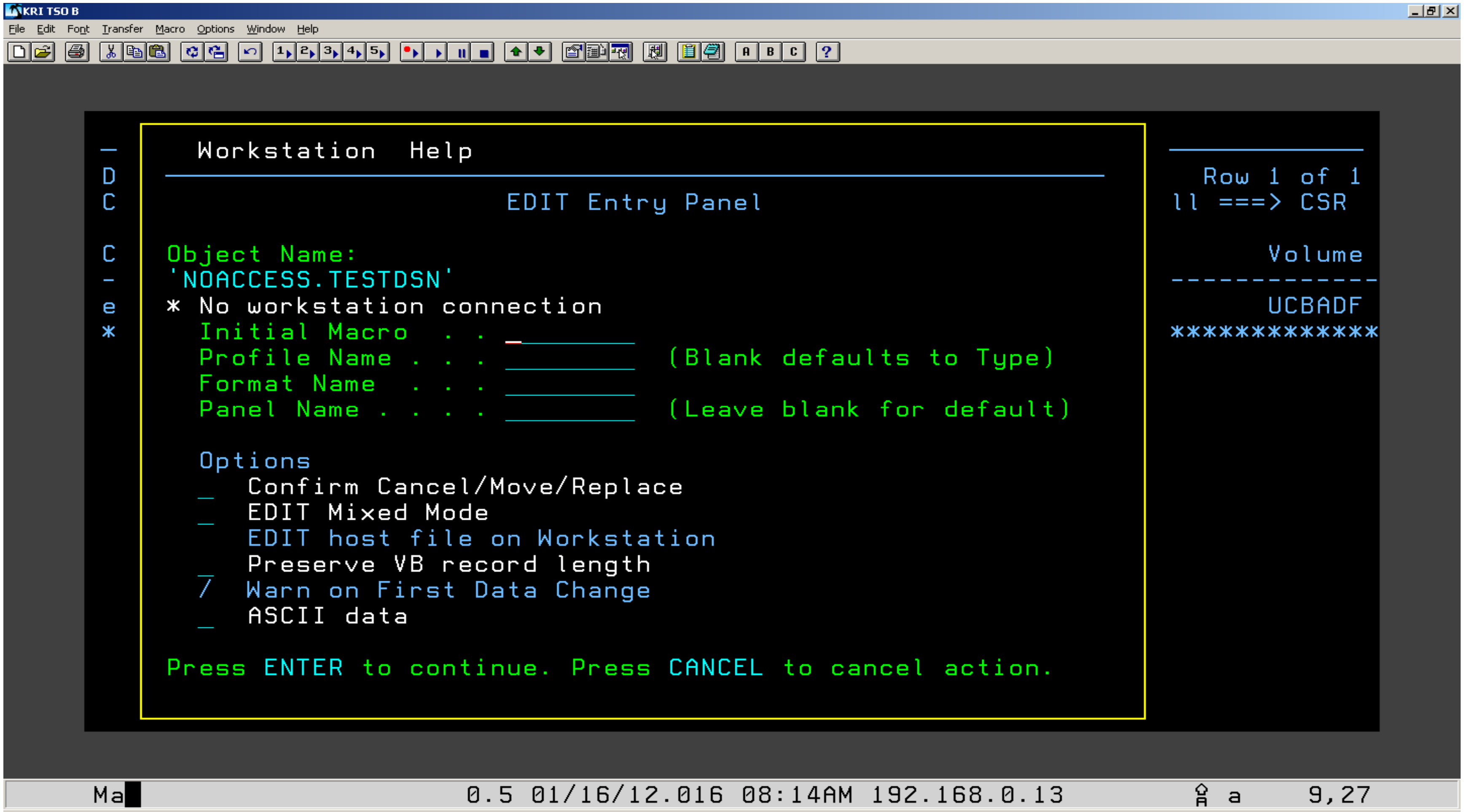
```
DSLIST - Data Sets Matching NOACCESS.TESTDSN                    Row 1 of 1
Command ===> ________________________________________________ Scroll ===> CSR

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

Demonstration - ISPF 3.4 Dataset List



```
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 ****************************
```

Demonstration - Getting into Edit

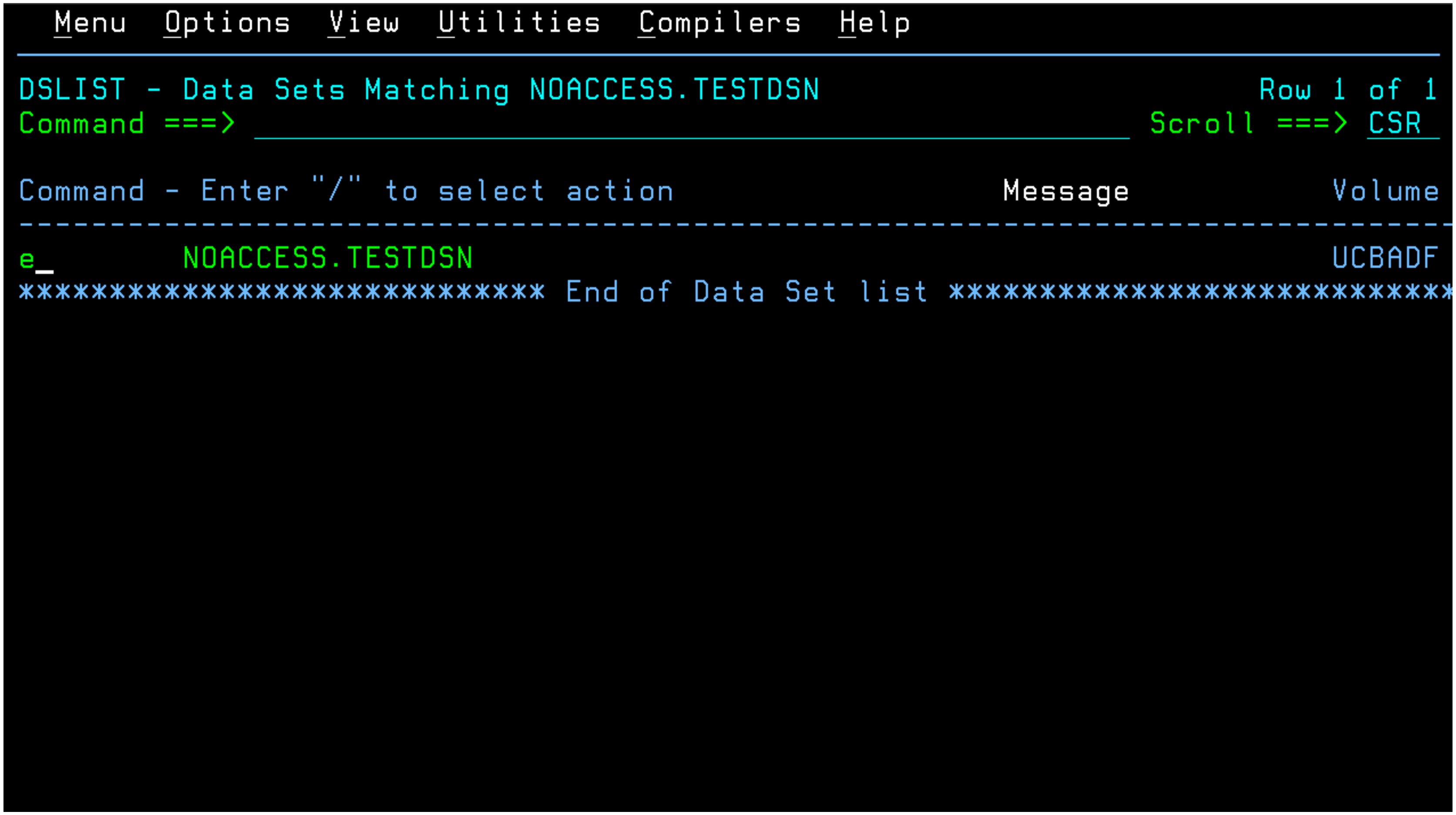


```
   Workstation  Help
 ──────────────────────────────────────────────────────────
                EDIT Entry Panel

Object Name:
'NOACCESS.TESTDSN'
* No workstation connection
  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.
```

```
  Row 1 of 1
ll ===> CSR

      Volume
-------------
      UCBADF
*************
```

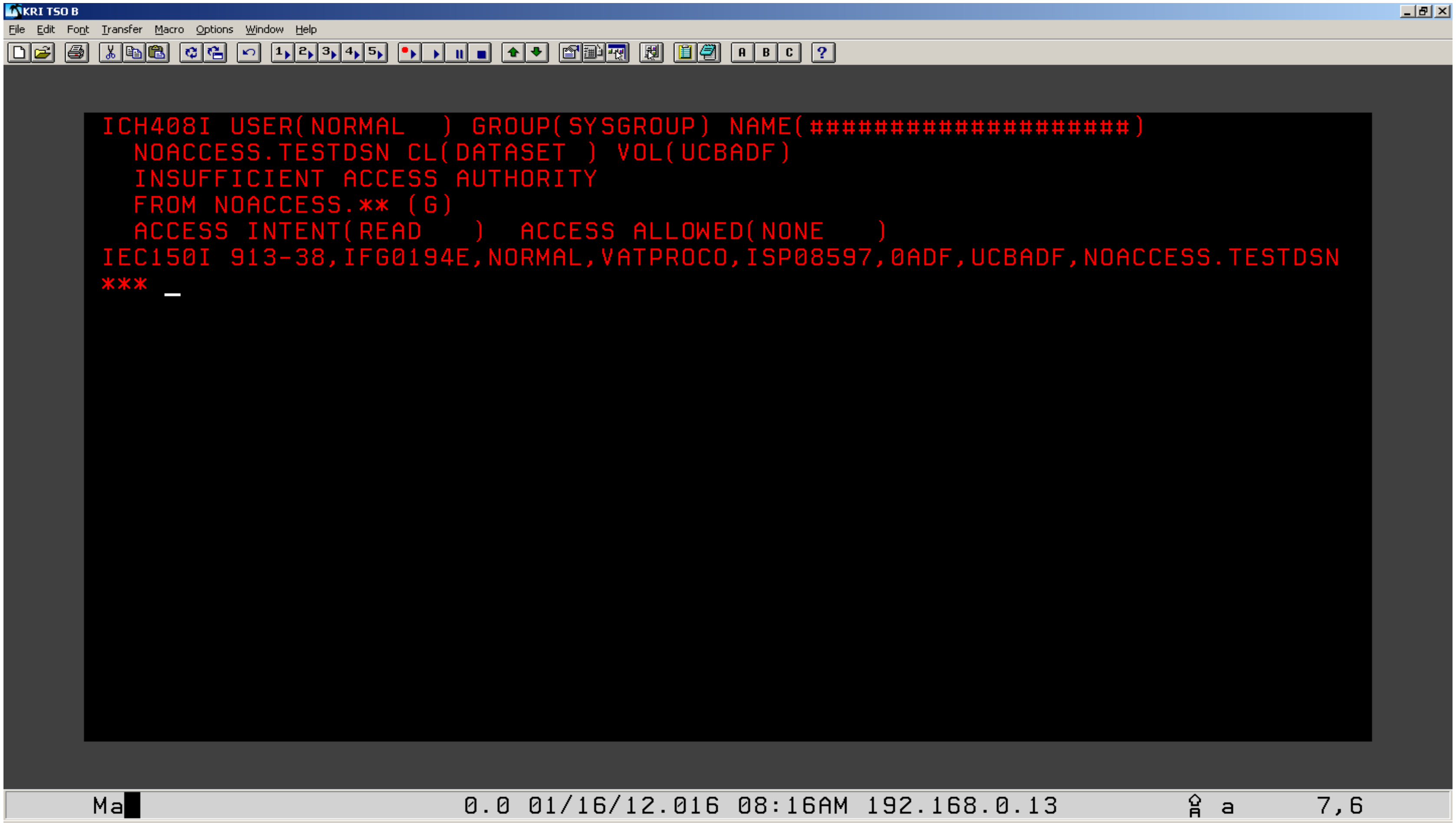
```
Ma      0.5 01/16/12.016 08:14AM 192.168.0.13      a     9,27
```

Demonstration - 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 ****************************
```

Demonstration - Access Denied!

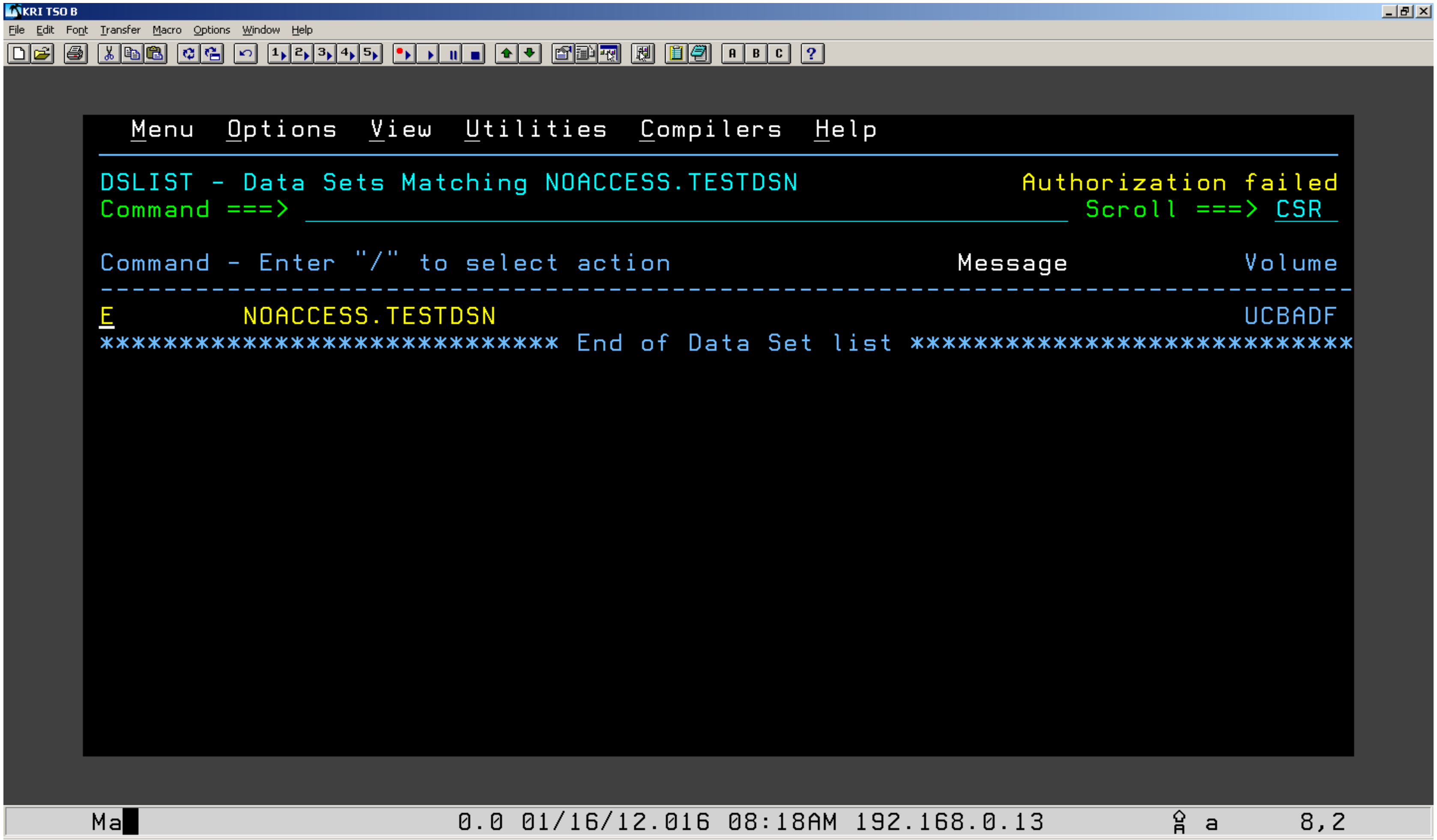


```
ICH408I USER(NORMAL   ) GROUP(SYSGROUP) NAME(####################)
  NOACCESS.TESTDSN CL(DATASET ) VOL(UCBADF)
  INSUFFICIENT ACCESS AUTHORITY
  FROM NOACCESS.** (G)
  ACCESS INTENT(READ   )  ACCESS ALLOWED(NONE   )
IEC150I 913-38,IFG0194E,NORMAL,VATPROCO,ISP08597,0ADF,UCBADF,NOACCESS.TESTDSN
***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

```
    Ma          0.0 01/16/12.016 08:16AM 192.168.0.13        a     7,6
```

key resources, inc.
Ensuring System Integrity For z/Series

Demonstration - User Could not Access Dataset

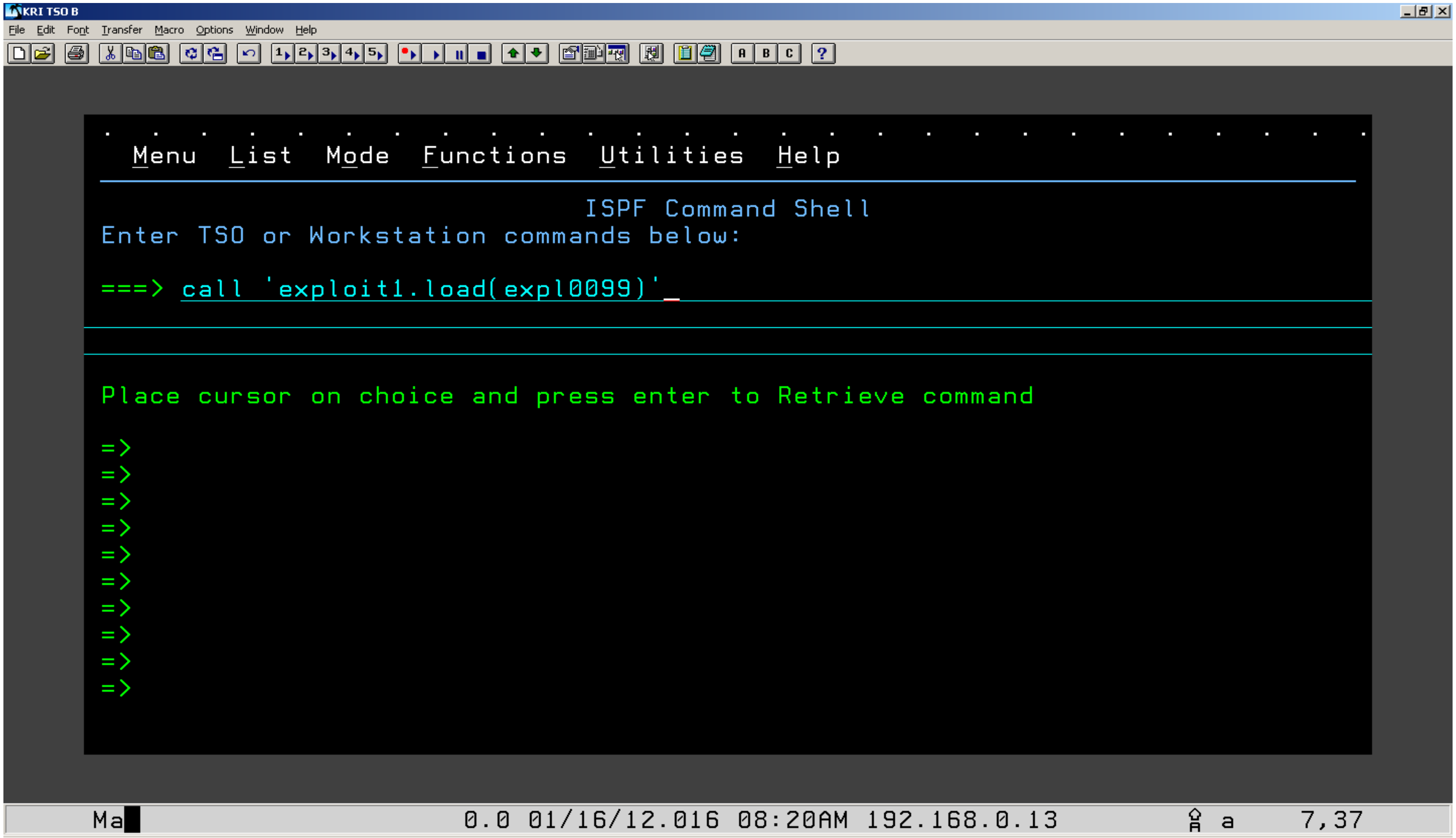


```
  Menu  Options  View  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 DSLIST - Data Sets Matching NOACCESS.TESTDSN              Authorization failed
 Command ===> ________________________________________________ Scroll ===> CSR

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

```
     Ma                    0.0 01/16/12.016 08:18AM 192.168.0.13       a      8,2
```

key resources, inc.
Ensuring System Integrity For z/Series

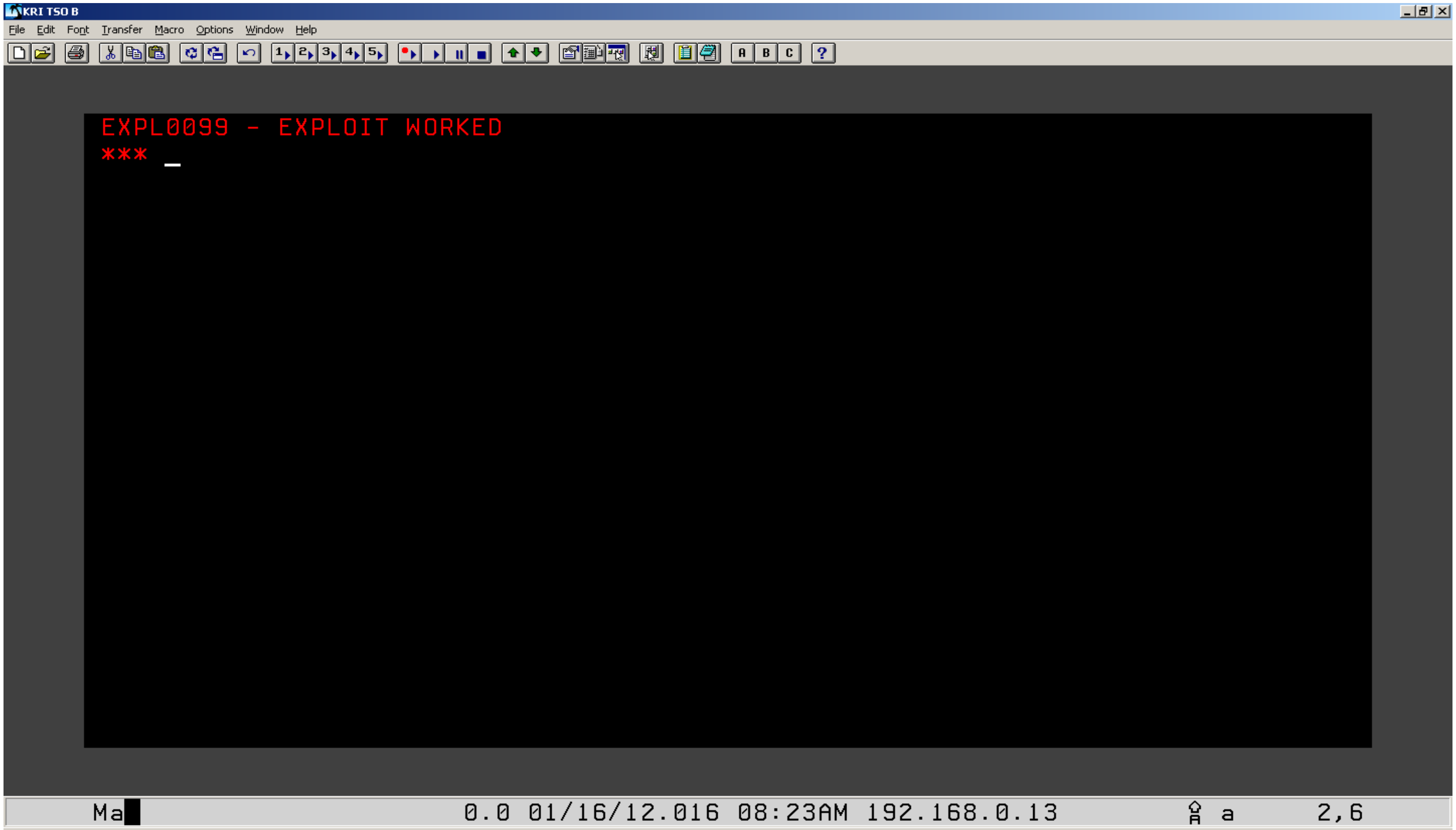
Demonstration - ISPF-6 - Run the Exploit



```
  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

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

    Ma          0.0 01/16/12.016 08:20AM 192.168.0.13           a     7,37
```

key resources, inc.
Ensuring System Integrity For z/Series

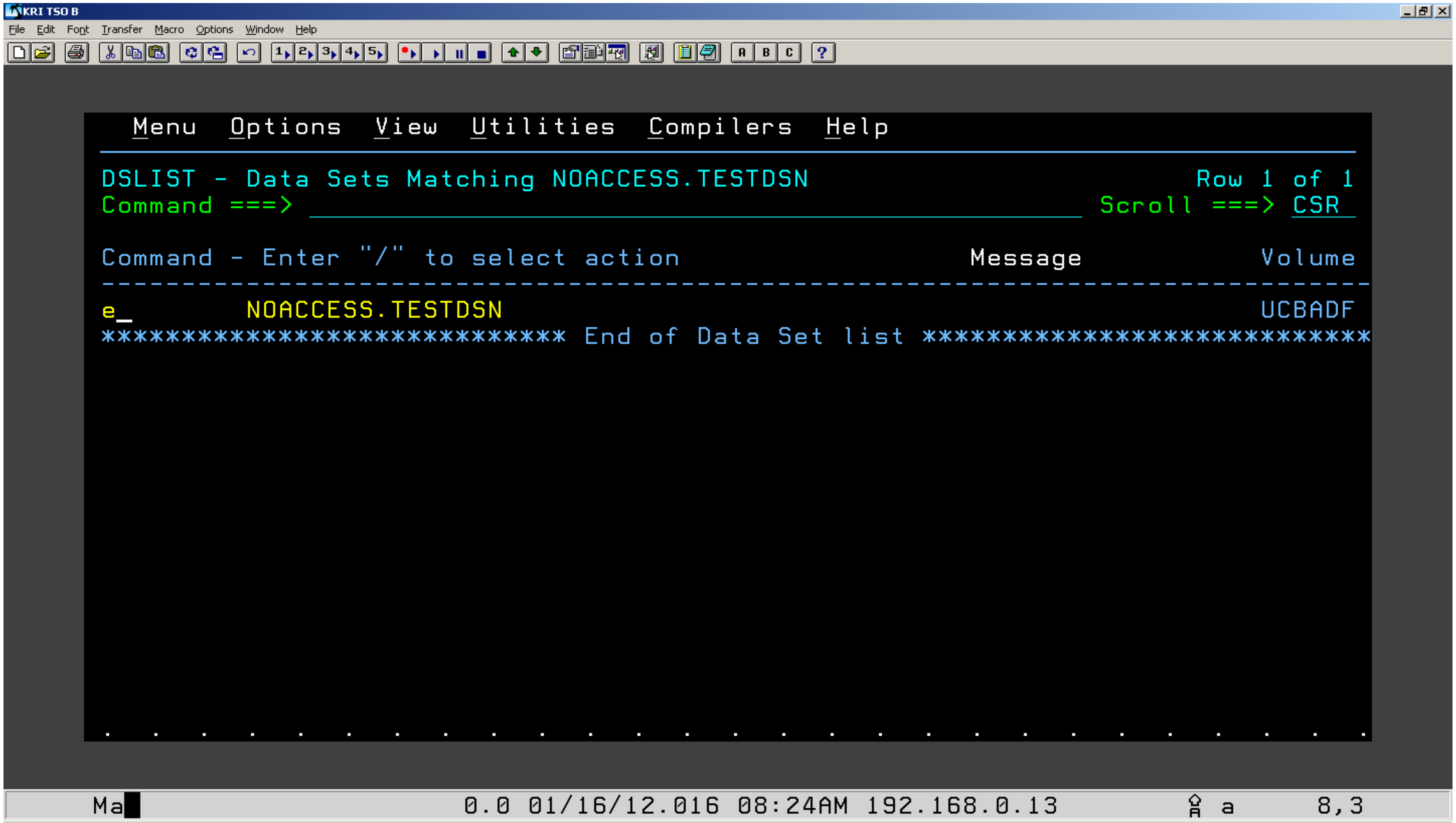
Demonstration - Exploit Successful!



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

```
Ma        0.0 01/16/12.016 08:23AM 192.168.0.13        a        2,6
```

Demonstration - Lets Try Again

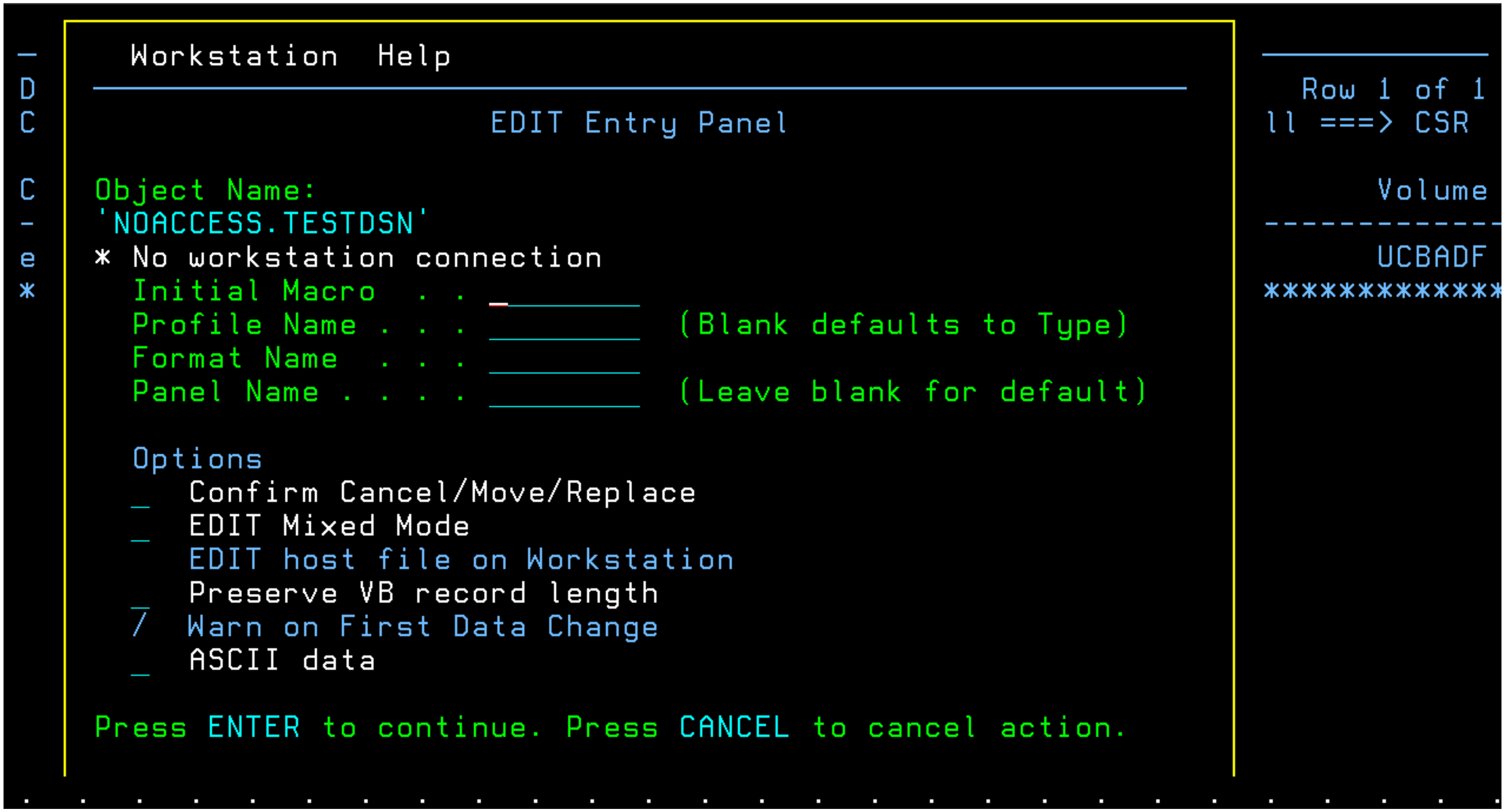


```
   Menu  Options  View  Utilities  Compilers  Help
 ------------------------------------------------------------------------------
 DSLIST - Data Sets Matching NOACCESS.TESTDSN                        Row 1 of 1
 Command ===> ________________________________________________  Scroll ===> CSR

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

```
     Ma          0.0 01/16/12.016 08:24AM 192.168.0.13          a      8,3
```

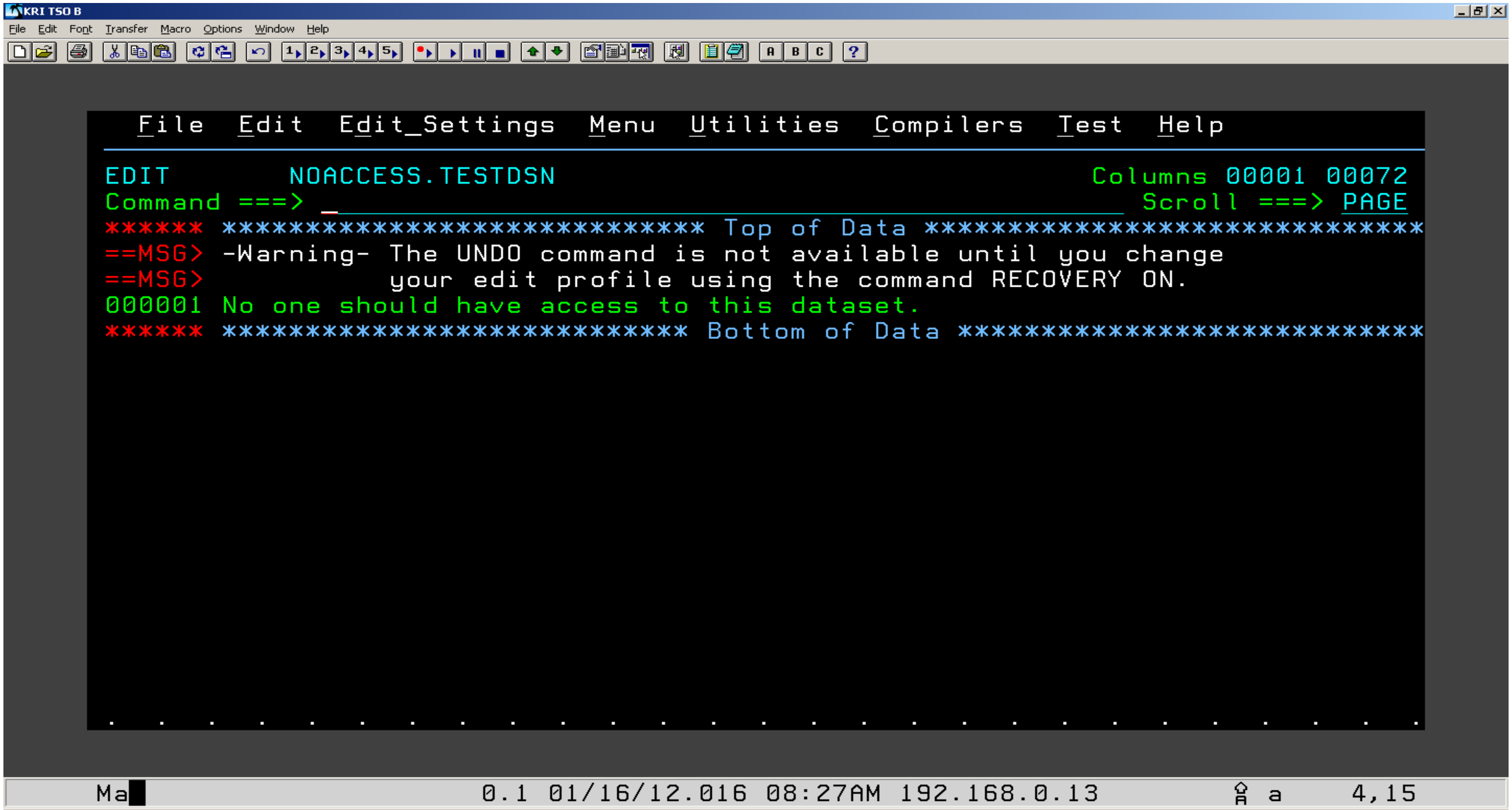
key resources, inc.
Ensuring System Integrity For z/Series

Demonstration - 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.
```

Demonstration - 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 ****************************
```

```
Ma          0.1 01/16/12.016 08:27AM 192.168.0.13          a     4,15
```

Demonstration - Let’s Review What Just Happened

- A demonstration of an exploit:
  - INTEGRITY based ALTER level vulnerability

- This exploit will allow **any** TSO user to:
  - **Compromise ALL data on your system**
  - **Compromise the System**

- This vulnerability can be exploited by batch users
- This vulnerability has a CVSS score of 8.4
- This is a compliance violation in every documented compliance guideline!

System Configuration Vulnerabilities

- IPL (or boot) parameters
- Subsystem startup (JES2|VTAM|TCPIP|CICS|….) parameters
- When specified incorrectly or dynamically modified may introduce vulnerabilities

Managing System Configuration Vulnerabilities

- Establish the parameters required for each system
  - Document the settings
  - Continuously monitor settings
- Document exceptions
- Remediate any discrepancies

Managing System Configuration Vulnerabilities

- Assign a CVSS score (or equivalent)
- Keep a history of problems
- Keep a history of changes (who|what|when|where|why)

External Security Manager (ESM)

- Controls the Security Implementation on your System(s)
- Critical to your Operations
- When specified incorrectly or dynamically modified may introduce vulnerabilities

Managing ESM Based Vulnerabilities (1)

- Establish which Parameters are Required for each system
- Document the settings
- Continuously monitor settings
- Document Exceptions

Managing ESM Based Vulnerabilities (2)

- Remediate any Discrepancies
- Calculate a CVSS score (or equivalent)
- Keep a history of problems
- Keep a history of changes (who|what|when|where|why)

Integrity Based Vulnerabilities

- z/OS has a Statement of Integrity
  - If an unauthorized user bypasses installation controls when not specifically allowed by the installation IBM will take steps to address the problem
- Unauthorized users should not be able to bypass the controls you (and z/OS) have in place
- In order for this to be true z/OS and all modifications made to z/OS (exits, ISV products, installation written code….) have to adhere to the IBM statement of integrity
- Integrity vulnerabilities exist on your system(s)

Managing Integrity Based Vulnerabilities (1)

- Ensure vendors that provide software for z/OS have an equivalent to the IBM statement of integrity
- Perform integrity based pen testing each time maintenance is applied OR when new versions are installed
- This penetration testing should be a normal part of your QA effort
- Calculate a CVSS score (or equivalent)

Managing Integrity Based Vulnerabilities (2)

- Patch management is required
- The installation cannot change configuration parameters to remediate the problem
- Only patches will remediate the vulnerabilities
- Need to monitor your systems to verify patches are applied
- More work required when migrating to new release
  - Are all old patches applied to source base of next release OR are new patches required

Integrity Assessment (1)

- Focus on authorized code paths
  - SVCs
  - PC routines
  - Exits
  - APF authorized programs

- There can be 10,000 + programs to review

Integrity Assessment (2)

For each vulnerability identified:

- Verify exploitability
- Collect information about the vulnerability
  - What program
  - How to invoke it
  - What parameters to pass
- Don’t create an exploit
  - Puts your installation at risk
  - Puts code owner at risk
  - Puts other installations at risk

Integrity Assessment (3)

For each vulnerability identified:

- Why you might have to create an exploit
  - Prove to installation
  - Code owner won’t work on problem without it
- Identify the Code Owner
- Calculate a CVSS score – ALTER level Integrity based vulnerabilities will normally be in the 8.4 range
- Report Problem and CVSS score to the Code Owner
- Code Owner Accepts the Problem

Integrity Assessment (4)

For each vulnerability identified:

- Code Owner makes Remediation Available
- Apply Remediation to your System
- You reassess the system to verify that remediation:
  - Fixes the Problem
  - Does not introduce any New Problems
- Do this until no more vulnerabilities
- Restart process next time you do maintenance or upgrade your system

Patch management for Integrity Vulnerabilities

- Remediation for Integrity Based Vulnerabilities will be a patch
- You need to ensure that patch is applied to all of your systems
- As you upgrade you need to make sure all patches have been applied in source for next release – if not then you will need patches for the next release
- Majority of Vulnerabilities found are Zero Day

Summary

z/OS is one of the most secure platforms however :

- Vulnerability scanning and Penetration testing must be done on your Mainframe
- Most if not all compliance standards call for one or the other
- Most concede the need for external network testing but testing of Internal access is needed as well
- You need to be performing patch management for the integrity patches

Questions?

Key Resources, Inc.

ray.overby@kr-inc.com

(312) KRI-0007

www.kr-inc.com