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: The Introduction

Agenda

- Introduction
- z/OS Security Basics
  - SAF
  - RACF, ACF2 & TSS
  - Resource Managers such as CICS, DB2, etc
- Hacking, Pen Testing and Ethical hacking, what's it all about?
- What is Vulnerability scanning?
- What are the Top Ten Audit issues seen?
- Is anyone interested in this stuff?
- Have mainframe systems ever been hacked?
- How have they been hacked?
- Questions

Introduction

Introduction

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

This is where Mark Lives!

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!

z/OS Security Basics

Reliability and Security

- A combination of z/OS Software and System z hardware can provide:
  - Confidentiality (not disclosure)
  - Integrity (not alteration)
  - Availability (not destruction)
- When configured correctly!
- Remember system z is no different to any other server if not configured correctly

Reliability and Security

- Buffer Overflow - not a real problem on z/OS
  - Address spaces and storage keys prevent applications from storing into someone else's storage
- Your ESM (RACF, ACF2 or TSS) can protect the complete system
  - All access to the system should require authentication with your ESM
  - A detailed audit trail can be created, but its optional
- Daemons are protected against modification and misuse
  - Security critical programs must run in a controlled environment
- TCP/IP stacks, ports and network addresses can be protected using your ESM
  - Can prevent rogue programs from taking over ports
  - Protects system and network from insider attacks, modification and misuse

RACF and z/OS Relationship

Assumption 1: Assumes the Resource Manager is calling!

Assumption 2: Assumes the Resource Manager does not override the decision made by RACF.

Based on Profiles! (User, Group, Resource)

MVS

RACROUTE Interface

RACF

RACF Database or In-Storage Copy

Assumption 3: Assumes correct/required profiles are defined to RACF?

Assumption 4: Assume the default RC set in the CDT does not allow access when RC4 (profile not defined) is handled as a RC0 (allow) versus RC8 (denied)

Assumption 5: Assume what is in storage is correct !

Hacking, Pen Testing and Ethical hacking:

what's it all about

Penetration Testing vs Hacking

- Who knows the difference?
- Well it depends on which way round you wear the baseball cap ☺
- The good guys do penetration testing aka ethical hacking
- The bad guys do hacking

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 minimize the risk of an attacker compromising your system
  - Basically we try to find holes in your system before somebody else does!

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..

What's typically done?

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

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.)

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

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!!

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…….

Why do a penetration test?

- Systems at various times have been delivered misconfigured or with misguided documentation
- Default configuration do not address “proper” security
- The effects of this misconfiguration and advice generally last until someone finds them
- Make sure that it’s you that finds these and not some-one else!

Why do a penetration test?

- Various ways to install new versions of z/OS have been used over time
- We tend to migrate our RACF database with the operating system
  - So a mistake made as far back as OS/390 2.10 may well be there on our RACF database at z/OS 1.13 or even 2.1!
- It is not uncommon for system parameters and/or Usermods to be copied to the latest z/OS release without a full appreciation of their impact

What is hacking?

- The same as the Penetration Test or Ethical Hack, but done by the bad guys and girls…
- The biggest difference is that they have plenty of time….
- We have seen some hacks perpetrated over a two year period!
- Quite often in the system z world its from the inside out…However, we have seen outside in attacks

What is vulnerability scanning?

What about z/OS Based Vulnerabilities?

- What is a vulnerability?
  - A weakness in z/OS systems, that allows the exploitation of products from Independent Software Vendor (ISV) and/or in-house developed authorized interfaces (SVCs and PCs) as well as (APF) authorised applications
- Vulnerabilities can compromise all data on your system as well as the system itself
  - Disrupt System Availability
  - View and Modify Sensitive Information
- It can allow an Internal attacker to circumvent RACF, ACF2 or Top Secret's installation controls

Exploiting a Vulnerability

- An Exploit is a way of taking advantage of a software Vulnerability
- Bypassing the installation-security controls
- Gain unauthorised access to data without proper permission and
- Without any logging (SMF)

Is anyone interested in this stuff?

Do we really care?

- Is anyone really interested in hacking mainframes?
- Take a look here:
  - http://mainframed767.tumblr.com/
- And some Interesting discussion on Linkedin
  - **Mainframe Security Gurus**
    - Discussion Started: IBM and CA Technologies Exploitable Code Found
    - Above Discussion Removed…no longer available
    - New Discussion Started: KRI's z/Assure VAP validates that CA Technologies has mitigated their ACF2 Code Vulnerability

Do we really care?

- Yes we do….

- The crown jewels of many organisations reside or originate from our mainframe systems

Have Mainframe systems ever been hacked

If so how was it done?

Can a Mainframe be hacked?

- Swedish Man Charged with Hacking IBM Mainframe & Stealing Money - Apr 16, 2013 -- Gottfrid Svartholm Warg was charged with hacking 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
- According to prosecutors, IBM mainframes belonging to Logica (who provide tax services to the Swedish government) and the bank were targeted in the attacks, which are said to have begun in 2010, and continued until April 2012
- A large amount of data from companies and agencies was taken during the hack, including a large amount of personal data, such as personal identity numbers...

Can a mainframe be hacked?

- An employee of a large UK Bank charged with defrauding the bank of £2,000,000 (Sterling)
- Jailed for 7 years
- So far only 50% has been recovered
- So can mainframes be hacked?
  - Yes they can…and we need to take steps to prevent this happening!

Summary

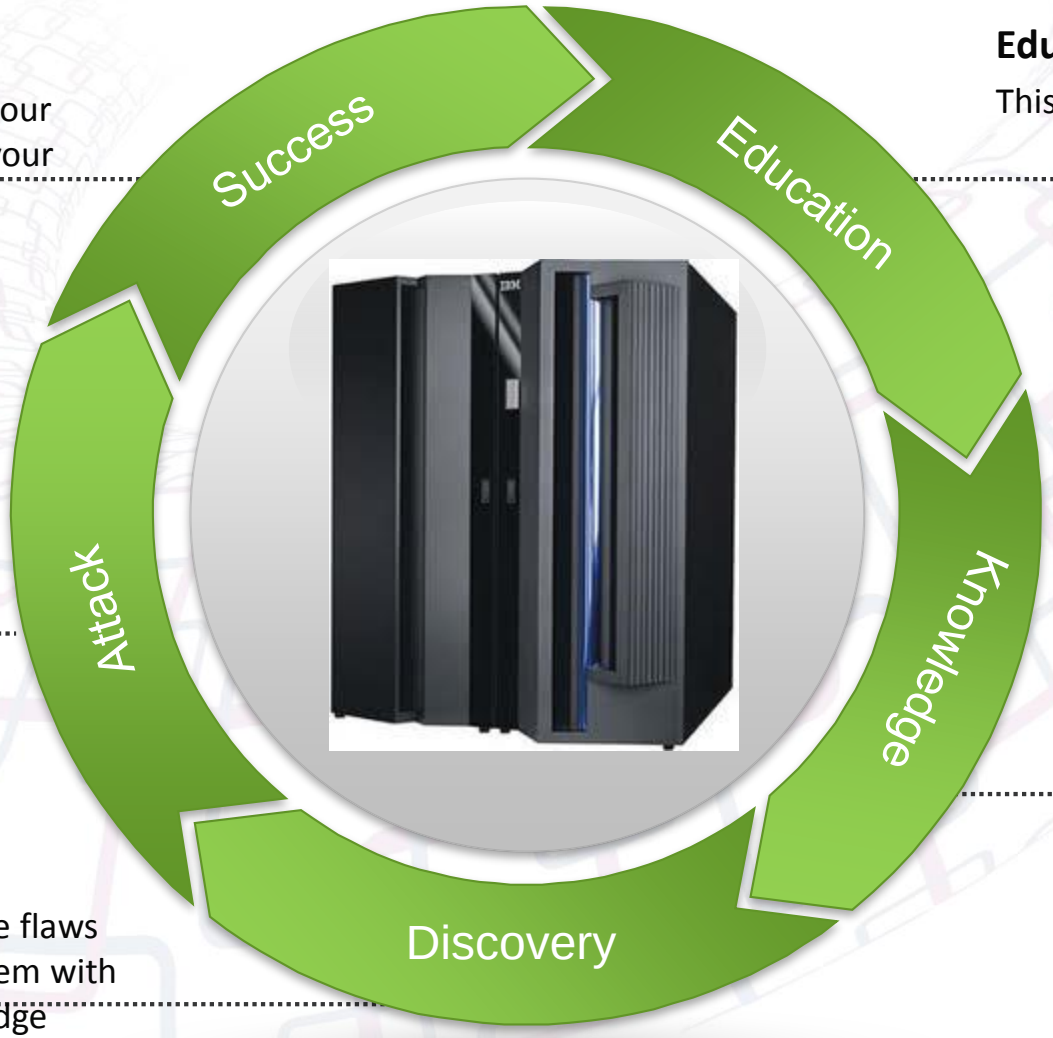
It’s a continuous process

Success?

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

Education

This session



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.

Summary

- Its not just about your ESM (RACF, ACF2 or TSS)
- You need a proactive security posture that checks and validates all of your security controls
- You need:
  - Audits
  - Penetration Testing/Ethical Hacking
  - Vulnerability Scanning
  - Education
- More importantly you need management and business support to be effective…..
- Otherwise you may end up in the evening news!

Questions

Contact Details

Mark Wilson
RSM Partners
markw@rsmpartners.com