# Penetration Testing

## Identifying vulnerabilities on the mainframe platform

## Introduction

As recognised experts in the mainframe security world, one of the many services RSM Partners offers its clients is **Penetration Testing.** This is a proven approach to identifying any security vulnerabilities that exist within a client's mainframe infrastructure.

Security vulnerabilities can lead to external or internal breaches of the existing security controls in place. Once breached, there is high risk of compromising the confidentiality, integrity and availability of the mainframe systems or the data residing thereon.

Such vulnerabilities seriously compromise the integrity of a mainframe system – hence why **IBM, under the terms and conditions of its warranty, clearly places responsibility for detection of any vulnerabilities upon its clients.**

Not surprisingly, it's also why PCI, Sarbanes Oxley and ISO standards stipulate that penetration testing needs to be carried out on a regular basis.

The RSM Partners **Penetration Testing** Service enables the proactive detection and reporting of any such vulnerabilities. Remedial steps can then be taken to prevent these vulnerabilities being exploited.

# The RSM Penetration Testing Service

Many people in the wider IT landscape believe the mainframe to be somewhat infallible to security breaches. However, while the mainframe is generally far more secure than any other platform out there, there are vulnerabilities that may be present – which obviously need to be identified and rectified.

Vulnerabilities come in two forms: **infrastructure related** and **software related**.

Infrastructure related vulnerabilities tend to arise from poor hardware configuration, poor system configuration parameters and poor security system controls.

Equally though, poor design and coding standards in either the z/OS operating system itself, Independent Software Vendor (ISV) products, or home-grown code can also create vulnerabilities.

Such vulnerabilities can be exploited - often via a simple REXX EXEC – presenting significant risk to the company.

Exploiting a vulnerability allows a basic user to gain control in a Privileged State - thereby gaining access to any resource they wish - without SMF records necessarily being generated. Once in an authorised state, the 'rogue' user can choose to: access sensitive data with ease; modify data at will; cause the system to operate abnormally; or even choose to crash the system - creating untold impact on the business.

The RSM **Penetration Testing** Service deploys senior technical skills and experience, operating on the client's systems, to identify any vulnerabilities that might be exploited.

Upon completion of the test, detailed reports are created listing all the vulnerabilities found.

The overall objective is to provide the client with assurances that any vulnerabilities that exist have been identified. These weaknesses can then be closed, preventing internal staff and/or third party applications from having a way of bypassing the security controls currently implemented.

A typical penetration test is split into three phases:

1. Non-Disruptive Data Collection
2. Penetration Testing
3. Software Scanning

## Non-Disruptive Data Collection

This phase is conducted onsite using a standard User ID. During this phase RSM attempts to gather some, if not all, of the following information:

- IPL Parameters for current IPL
- APF Authorised, Linklisted and LPA Datasets
- JES Spool & Checkpoint Datasets
- Page & SMF Datasets
- IPLPARM & Parmlib Datasets
- Hardware Configuration including IODF Datasets
- ISPF Datasets (CLIST, REXX, etc.)
- Security Information for all of the above (RACF, ACF2 & TSS)

## Penetration Testing

This phase is conducted onsite and using the User ID's supplied by the client.

During this phase RSM probes the system, determining if it is possible to elevate privileges.

The areas covered will include some, if not all, of the following:

- Library Access Checks
- Password Checks
- Public Dataset Checks
- Public Resource Checks
- User SVC Checks
- MVS & JES2 / JES3 Command Authority Checks
- RACF/TSS/ACF2 Exit Checks
- JES2 / JES3 Spool Dataset Checks
- MVS Subsystem Checks (IMS, DB2, CICS, NETView, etc.)
- MVS UNIX Environment Checks
- Miscellaneous Checks

## Software Scanning

The RSM Vulnerability Scanning software, operating on the client's systems, uses proprietary "fuzzy logic" technology to identify system integrity exposures found in Supervisor Call (SVC) Interfaces, Operating System Exits, Program Call (PC) Routines and Authorised Program Function (APF) calls.

Upon completion of a scan, the Vulnerability Scanning software collects code vulnerability data and generates a detailed report, listing the identified vulnerabilities.

These vulnerabilities can then be discussed with IBM, the ISVs and the installation's own software development teams, targeting prompt remediation of any and all issues identified.

# Administration Considerations

## Assumptions

1. RSM consultants will be on-site during the exercise
2. RACF, ACF2 or Top Secret is currently deployed
3. RSM will be allowed to install, customise, and run software tools to carry out the scanning
4. The mainframe image that RSM will have access to, will be a full clone of the production image (target system)
5. RSM consultants on-site will have access to:
    a. Appropriate facilities i.e. access to a desk/ terminal/phone
    b. The ESM system where the scanning is to be done
    c. A designated point of contact (project manager) for the project
    d. Appropriate allocation of time from client's personnel to support the activities
    e. Client personnel, suitably authorised to make any necessary security decisions
    f. Systems programming personnel who will be able to provide information about:
        i. system configuration parameters
        ii. ISV products installed
        iii. locally installed authorised programs
        iv. operating system exits

## Meetings

The following on-site meetings will be held:

- **Initial kick-off meeting:** The objective of this meeting is to introduce RSM consultants to relevant personnel on-site who will be participating in the project - to set goals and level set, reviewing any changes that have occurred since previous discussions. Various aspects relating to the engagement are discussed with a view to ensuring successful and timely project completion
- **Mid-week meeting:** To report on progress
- **Completion/Departure meeting:** To discuss findings

## System access

RSM Partners will require:

- Access to the target z/OS system: 2 TSO User IDs
- Each User ID will need to be able to:
    - Allocate datasets under the TSO User ID
    - Submit batch jobs
    - To see and delete these jobs using SDSF or similar product
    - Have **NO** security privileges (SPECIAL, AUDITOR, ETC)
- Security for the test IDs: since the data produced by this exercise is highly sensitive, only suitably authorised personnel should have access to the files created by these User IDs. All other access should be "NONE".
- RSM will install (client may wish to do this in advance) and customise the vulnerability scanning software. It is important that access to the system is provided on the morning of the first day that RSM consultants are on-site. Failure to do this could cause the assessment not to be completed in the allotted time. It typically takes up to 2 hours to install and customise the software. The target system must have CSA/SQA tracking turned on at IPL time.

## Deliverables

RSM will produce:

- **A Penetration Test Report**
- **Initial findings will be provided on the last day RSM consultants are on site**
- **The final report will be provided within two weeks of completing the on-site exercise**
- **Optionally, a demonstration of an exploit can be provided**
- **A check list for recommended client activities after the assessment completed**

Additional time is also allowed for RSM consultants interacting with vendors or internal staff, as necessary, helping them better understand the vulnerabilities identified.

## Timeline

RSM anticipates the data gathering, penetration testing, software scanning and analysis of a single image to take 10 working days elapsed time, consisting of 20 man days' effort.

The final report on findings is made available within two weeks of leaving the client site.

Clearly, if any highly significant security failings are identified, RSM will inform the client at the earliest opportunity so that corrective actions can be immediately initiated.

The presentation and follow up discussion on findings and the final report are delivered at a mutually convenient time.

# About RSM Partners

RSM Partners leads the way with its specialised focus on the IBM System z platform, delivering independent high calibre expertise and advice spanning the z/OS operating system, the various subsystems and associated middleware - as well as the network and associated hardware.

Over the years, RSM has become a valuable ally to many in the System z arena. Consistently and reliably delivering a quality approach - whether specific skills or managed projects; technical consultancy; support services; or niche solutions around security and cost reduction.

Highly regarded across the industry, both by vendors and clients alike, RSM Partners is also renowned for its assured handling of migrations as well as the implementation and leveraging of both IBM and third party z software.

RSM offerings currently include:

- Ad Hoc Specialist Skills
- Project Out-Tasking
- Technical Consultancy
- Security Related Services
- Software & Storage Migrations
- Cost Reduction & Performance Optimisation
- Managed, Hosted & DR Services
- 24*7 Support Contracts

Business Partner IBM

Business Partner IBM
Ready for Security Intelligence


To find out more about these and other RSM Partners services, call **+44 (0) 1527 837767** or visit **www.rsmpartners.com**

**T** +44 (0) 1527 837767 | **E** info@rsmpartners.com | **www.rsmpartners.com**

RSM PARTNERS
MAINFRAME

16_0252 - 11/10/V01