

Penetration Testing

Identifying vulnerabilities and security risks on the mainframe platform

INTRODUCTION

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

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 the 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.

BMC Mainframe Services penetration testing service enables the proactive detection and reporting of any such vulnerabilities to help prevent them from being exploited.

WHAT VULNERABILITIES DO MAINFRAMES HAVE?

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 IBM® z/OS® operating system itself, independent software vendor (ISV) products, or homegrown code can also create vulnerabilities. Such vulnerabilities can often be exploited via a simple REXX EXEC, presenting a 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 authorized 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 an untold impact on the business.

HOW TESTS ARE PERFORMED

Our 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 using a standard user ID. During this phase, BMC Mainframe Services attempts to gather some, if not all, of the following information:

- IPL parameters for current IPL
- APF-authorized, linklisted, and LPA datasets
- JES spool and checkpoint datasets
- Page and SMF datasets

- IPLPARM and Parmlib datasets
- Hardware configuration, including IODF datasets
- ISPF datasets (CLIST, REXX, etc.)
- Security information for all of the above
IBM® RACF®, CA ACF2™, CA Top Secret® (TSS)

Penetration testing

This phase is conducted using the user IDs supplied by the client.

During this phase, BMC Mainframe Services 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 supervisor call (SVC) checks
- IBM® MVS™ and JES2/JES3 command authority checks
- RACF/TSS/ACF2 exit checks
- JES2/JES3 spool dataset checks
- MVS subsystem checks (IBM® IMS®, IBM® Db2®, IBM® CICS®, IBM® NetView®)
- MVS UNIX environment checks
- Miscellaneous checks

Software scanning

Our 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 authorized 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. RACF, ACF2, or Top Secret is currently deployed
2. BMC Mainframe Services will be allowed to install, customize, and run software tools to carry out the scanning

3. The mainframe image that BMC Mainframe Services will have access to will be a full clone of the production image (target system)
4. BMC Mainframe Services consultants will have access to:
 - Appropriate facilities i.e., a desk/terminal/phone
 - The external security manager (ESM) system where the scanning is to be done
 - A designated point of contact (project manager) for the project
 - Appropriate allocation of time from the client's personnel to support the activities
 - Client personnel, suitably authorized to make any necessary security decisions
 - Systems programming personnel who will be able to provide information about:
 - » System configuration parameters
 - » ISV products installed
 - » Locally installed authorized programs
 - » Operating system exits

Meetings

The following meetings will be held:

- **Initial kick-off meeting:** The objective of this meeting is to introduce BMC Mainframe Services consultants to relevant personnel 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 to ensure successful and timely project completion
- **Mid-point meeting:** To report on progress
- **Completion/departure meeting:** To discuss findings

System access

BMC Mainframe Services will require:

- Access to the target z/OS system: Two TSO user IDs
- Each User ID will need to be able to:
 - » Allocate datasets under the TSO user ID
 - » Submit batch jobs
 - » See and delete these jobs using System Display and Search Facility (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 authorized personnel should have access to the files created by these user IDs. All other access should be "NONE".

- BMC Mainframe Services will install and customize the vulnerability scanning software. It is important that access to the system is provided on the morning of the first day that BMC Mainframe Services consultants begin testing. Failure to do this could cause the assessment not to be completed in the allotted time. It typically takes up to two hours to install and customize the software. The target system must have CSA/SQA tracking turned on at IPL time.

DELIVERABLES

BMC Mainframe Services will produce:

- A penetration test report
- A report of initial findings
- The final report will be provided within two weeks of completing the exercise
- Optionally, a demonstration of an exploit can be provided
- A checklist for recommended client activities after the assessment is completed

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

TIMELINE

BMC Mainframe Services anticipates the data gathering, penetration testing, software scanning, and analysis of a single image to take ten working days elapsed time, consisting of 20 person-days' effort.

The final report on findings is made available within two weeks of testing completion.

If any highly significant security failings are identified, BMC Mainframe Services 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 BMC MAINFRAME SERVICES

BMC Mainframe Services leads the way with its specialized focus on the IBM® System z® platform, delivering independent high caliber 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, BMC Mainframe Services has become a valuable ally to many in the System z arena, consistently and reliably delivering a quality approach, whether customers need specific skills, managed projects, technical consulting, support services, or niche security and cost reduction solutions.

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

BMC Mainframe Services offerings currently include:

- Ad hoc specialist skills
- Project out-tasking
- Technical consultancy
- Security-related services
- Software and storage migrations
- Cost reduction and performance optimization
- Managed, hosted and disaster recovery services
- 24/7 support contracts



FOR MORE INFORMATION

To learn more about The BMC Mainframe Services Penetration Testing, please visit:

bmc.com/mainframe-services

About BMC

From core to cloud to edge, BMC delivers the software and services that enable over 10,000 global customers, including 84% of the Forbes Global 100, to thrive in their ongoing evolution to an Autonomous Digital Enterprise.

BMC—Run and Reinvent

www.bmc.com



BMC, the BMC logo, and BMC's other product names are the exclusive properties of BMC Software, Inc. or its affiliates, are registered or pending registration with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other trademarks or registered trademarks are the property of their respective owners. © Copyright 2021 BMC Software, Inc.

