Mainframe Virtual User Groups

VIRTUAL DB2 USER GROUP

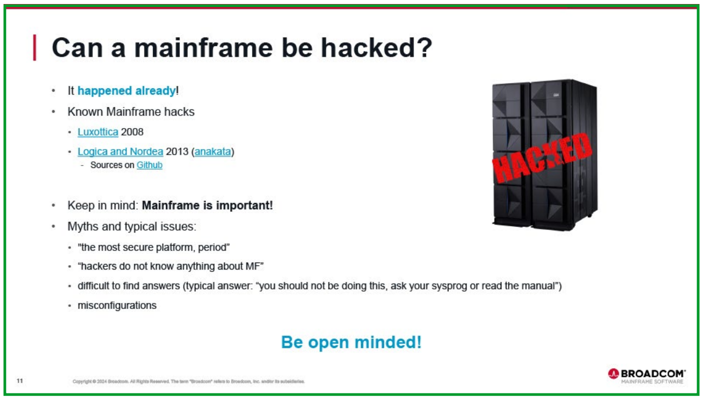
NEWSLETTER 10 | JUNE 2024

Virtual Db2 User Group Presentation

Unveiling the security landscape: Can Db2 be hacked?

In May, the Mainframe Virtual User Group for Db2 met for "Can Db2 be hacked? Yes, sure it can.", a session supported by IntelliMagic. The speaker, Emil Kotrc, is an experienced Principal Software Architect with a rich background in the computer software industry, particularly in IBM Db2 and agile methodologies. He holds a PhD in Mathematical Engineering from Czech Technical University in Prague and is an active member of the International Db2 User Group (IDUG) Content Committee.

Kotrc began by establishing the reality that, contrary to the long-held belief of mainframes being impervious to attacks, they can indeed be hacked if not properly secured. He cited historical incidents and discussed the misconceptions that often lead to a false sense of security. The core message was clear: while mainframes are inherently secure, they require diligent and continuous security practices to maintain this status.



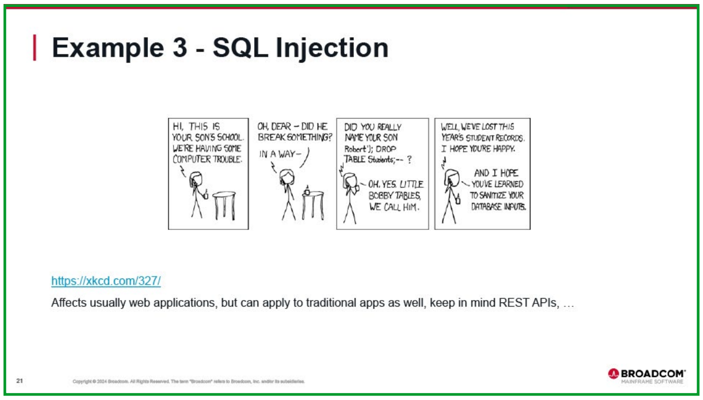
Can a mainframe be hacked?

- It **happened already**!
- Known Mainframe hacks
  - Luxottica 2008
  - Logica and Nordea 2013 (anakata)
    - Sources on Github
- Keep in mind: **Mainframe is important!**
- Myths and typical issues:
  - "the most secure platform, period"
  - "hackers do not know anything about MF"
  - difficult to find answers (typical answer: "you should not be doing this, ask your sysprog or read the manual")
  - misconfigurations

Be open minded!

11 Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

One of the key highlights of Kotrc's presentation was his explanation of various hacking techniques that can compromise Db2 systems. He outlined three primary scenarios: privilege escalation, unauthorized data access, and SQL injection. Each example was meticulously detailed, demonstrating how an attacker could exploit specific vulnerabilities. For instance, he showed how improper handling of APF-authorized libraries could allow an attacker to escalate privileges and gain unauthorized access to sensitive data.



Example 3 - SQL Injection

HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

https://xkcd.com/327/

Affects usually web applications, but can apply to traditional apps as well, keep in mind REST APIs, …

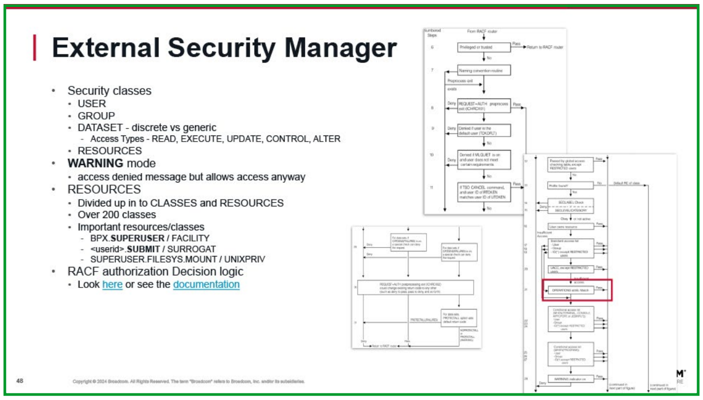
21 Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

BROADCOM
MAINFRAME SOFTWARE

Kotrc also emphasized the importance of understanding the distinction between authentication and authorization within the Db2 environment. He explained how Db2 handles user authentication and the role of authorization in controlling access to Db2 resources. This distinction is crucial for setting up effective security measures, as it helps in identifying potential weak points in the system.

Unveiling the security landscape: Can Db2 be hacked?
Continued

Additionally, Kotrc highlighted the significance of external security managers (ESMs) like RACF in managing Db2 security. He discussed how ESMs can be configured to control access to Db2 resources and the potential pitfalls if they are not properly set up. The integration of ESMs with Db2's internal security mechanisms was presented as a robust approach to enhancing overall system security.

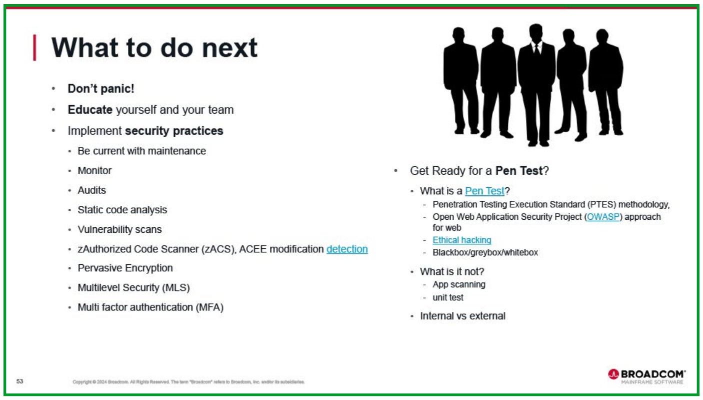


External Security Manager

- Security classes
  - USER
  - GROUP
  - DATASET - discrete vs generic
    - Access Types - READ, EXECUTE, UPDATE, CONTROL, ALTER
  - RESOURCES
- **WARNING** mode
  - access denied message but allows access anyway
- RESOURCES
  - Divided up in to CLASSES and RESOURCES
  - Over 200 classes
  - Important resources/classes
    - BPX.**SUPERUSER** / FACILITY
    - <userid>.**SUBMIT** / SURROGAT
    - SUPERUSER.FILESYS.MOUNT / UNIXPRIV
- RACF authorization Decision logic
  - Look here or see the documentation

48 Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Towards the end of his presentation, Kotrc provided recommendations for preventing security breaches. He advocated for a multi-faceted approach that includes regular security scans, penetration testing, and adherence to industry benchmarks such as those provided by the Center for Internet Security (CIS). He also stressed the importance of educating both security teams and end-users about potential vulnerabilities and best practices for maintaining security.



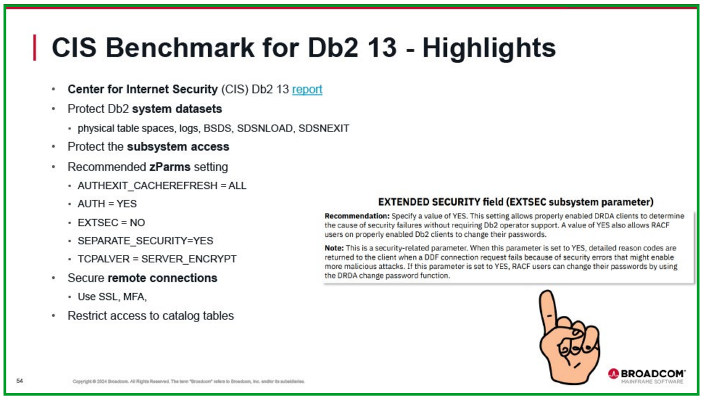
What to do next

- **Don't panic!**
- **Educate** yourself and your team
- Implement **security practices**
  - Be current with maintenance
  - Monitor
  - Audits
  - Static code analysis
  - Vulnerability scans
  - zAuthorized Code Scanner (zACS), ACEE modification detection
  - Pervasive Encryption
  - Multilevel Security (MLS)
  - Multi factor authentication (MFA)
- Get Ready for a **Pen Test**?
  - What is a Pen Test?
    - Penetration Testing Execution Standard (PTES) methodology,
    - Open Web Application Security Project (OWASP) approach for web
    - Ethical hacking
    - Blackbox/greybox/whitebox
  - What is it not?
    - App scanning
    - unit test
  - Internal vs external

53 Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

BROADCOM MAINFRAME SOFTWARE

In conclusion, Emil Kotrc's presentation was a comprehensive overview of the vulnerabilities and security practices associated with Db2 for z/OS. By shedding light on the potential risks and providing actionable insights, Kotrc equipped his audience with the knowledge needed to better secure their Db2 environments. For mainframe professionals, this presentation serves as a valuable resource in the ongoing effort to safeguard critical systems against cyber threats.



CIS Benchmark for Db2 13 - Highlights

- **Center for Internet Security** (CIS) Db2 13 report
- Protect Db2 **system datasets**
  - physical table spaces, logs, BSDS, SDSNLOAD, SDSNEXIT
- Protect the **subsystem access**
- Recommended **zParms** setting
  - AUTHEXIT_CACHEREFRESH = ALL
  - AUTH = YES
  - EXTSEC = NO
  - SEPARATE_SECURITY=YES
  - TCPALVER = SERVER_ENCRYPT
- Secure **remote connections**
  - Use SSL, MFA,
- Restrict access to catalog tables

EXTENDED SECURITY field (EXTSEC subsystem parameter)

Recommendation: Specify a value of YES. This setting allows properly enabled DRDA clients to determine the cause of security failures without requiring Db2 operator support. A value of YES also allows RACF users on properly enabled Db2 clients to change their passwords.

Note: This is a security-related parameter. When this parameter is set to YES, detailed reason codes are returned to the client when a DDF connection request fails because of security errors that might enable more malicious attacks. If this parameter is set to YES, RACF users can change their passwords by using the DRDA change password function.

54 Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

BROADCOM MAINFRAME SOFTWARE

Access the Recording

- Sponsorship opportunity—We are looking for additional co-sponsors for the Virtual Db2 user group. The user group has been in existence since 2022 and is gaining respect among users of Db2. The user group gives its sponsors an opportunity to show that they are working with, and helping to build, the Db2 user community. Contact virtualusergroups@gmail.com for more information.
- Save the date for our next session on July 16.

About the Virtual Db2 User Group

The Virtual Db2 user group is an independently-operated vendor-neutral site run by and for the mainframe Db2 user community. This is a mainframe Db2 information website, not in any way related to, sponsored, or approved by IBM, which is the legitimate owner of the trademark, and any use of the mark in the URL or the body of the site is for information, education, and opinion expression purposes. The Virtual Db2 user group was established as a way for individuals using IBM's Db2 for z/OS database to exchange information, learn new techniques, and advance their skills with the product. Anyone with an interest in Db2 for z/OS is welcome to join the Virtual Db2 user group and share in the knowledge exchange.

SPONSORS

IntelliMagic
Availability Intelligence