IBM System z – 7th European GSE / IBM Technical University for z/VSE, z/VM and Linux on System z

VS05 Hints und Tipps

Heinz Peter Maassen (hp.maassen@lattwein.de) *Lattwein GmbH*

Ingolf Salm (salm@de.ibm.com) *IBM Deutschland GmbH*

Trademarks

The following are trademarks of the International Business Machines Corporation in the United States, other countries, or both.

Not all common law marks used by IBM are listed on this page. Failure of a mark to appear does not mean that IBM does not use the mark nor does it mean that the product is not actively marketed or is not significant within its relevant market.

Those trademarks followed by ® are registered trademarks of IBM in the United States; all others are trademarks or common law marks of IBM in the United States.

For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml:

*, AS/400®, e business(logo)®, DBE, ESCO, eServer, FICON, IBM®, IBM (logo)®, iSeries®, MVS, OS/390®, pSeries®, RS/6000®, S/30, VM/ESA®, VSE/ESA, WebSphere®, xSeries®, z/OS®, zSeries®, z/VM®, System i, System i5, System p, System p5, System x, System z, System z9®, BladeCenter®

The following are trademarks or registered trademarks of other companies.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.
Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.
Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.
Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.
UNIX is a registered trademark of The Open Group in the United States and other countries.
Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.
ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.
IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency, which is now part of the Office of Government Commerce.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

Übersicht

- Sind Ihre Daten noch sicher?
  - Einige letzte Meldungen
- Email und Verschlüsselung
- Schutz von aussen
- Schwachstellen
- Wie ist Datensicherheit mit z/VSE möglich

Einige letzte Meldungen

Das haben Betroffene des Datendiebstahls zu befürchten

13.09.2013, 13:42 Uhr | Sebastian Weber, dpa

Hacker haben Datensätze Vodafone-Kunden gestohlen. Viel anfangen können sie damit aber nicht. (Quelle: Sabine Gudath/sepp spiegl/Montag/imago)

Name, Geburtsdatum, Kontonummer und Bankleitzahl sowie Geschlecht des Kunden, diese Daten haben Hacker von Vodafone erbeutet, wie das Unternehmen am Donnerstag mitteilte. Etwa zwei Millionen Kunden sind betroffen. Doch welchen Schaden können die Verbrecher mit diesen Informationen anrichten?

http://www.t-online.de/computer/sicherheit/id_65433464/vodafone-gesteht-datendiebstahl-was-kunden-zu-befuerchten-haben.html

Einige letzte Meldungen

Search DW

THEMEN MEDIA CENTER PROGRAMM DEUTSCH LERNEN

DEUTSCHLAND WELT WIRTSCHAFT KULTUR GLOBALE ZUSAMMENARBEIT WISSEN & UMWELT SPORT

THEMEN

INTERNET

Hackerangriff auf New York Times

Unterstützer des syrischen Machthabers Assad haben die Internetseite der "New York Times" lahmgelegt. Die Hackergruppe SEA bekannte sich zu dem Angriff. Sie hatte auch schon einen Twitter-Account von DW.de gestört.

Zwei Wochen nach Serverproblemen bei der New York Times hat ein Hackerangriff die

Datum 28.08.2013

Teilen Versenden
Facebook Twitter
google+ mehr ...

Schicken Sie uns Ihr Feedback!

Drucken Seite drucken

Permalink http://dw.de/p/19XeW

Die Top-Themen in drei Minuten

Das Journal der DW präsentiert die wichtigsten Nachrichten - aktuell, kurz

`http://www.dw.de/hackerangriff-auf-new-york-times/a-17050652`

Einige letzte Meldungen

Überwachungs- und Spionageaffäre 2013

Die **Überwachungs- und Spionageaffäre 2013** bezieht sich auf Enthüllungen von als Top Secret gekennzeichneten Dokumenten der National Security Agency (NSA) und darauf folgend weiterer Veröffentlichungen. Der US-amerikanische Whistleblower Edward Snowden enthüllte Anfang Juni 2013, wie die Vereinigten Staaten und das Vereinigte Königreich seit spätestens 2007 in großem Umfang die Telekommunikation und insbesondere das Internet global und verdachtsunabhängig überwachen und die so gewonnenen Daten auf Vorrat speichern. Auch Gebäude und Vertretungen der Europäischen Union sollen mit Hilfe von Wanzen ausspioniert worden sein. Im Verlauf der Affäre berichteten Medien über ähnliche Aktivitäten von weiteren Staaten. . . .

Edward Snowdon rüttelte die Politik wach. Was macht die IT heute nach den Meldungen anders?

http://de.wikipedia.org/wiki/Überwachungs-_und_Spionageaffäre_2013

Email und Verschlüsselung

- Herkömmliche E-Mails sind mit einer Postkarte vergleichbar.
- Der Inhalt liegt offen und kann von jedem mitgelesen werden.
- Auch beim Mail Dienstleister lassen sich die E-Mail Daten sogar einfach und automatisch per Programm auswerten oder als Kopie aufbewahren zur späteren Analyse.

Email und Verschlüsselung

- E-Mail ersetzt heute immer häufiger den Brief, Telegramm, Fernschreiben und Teletex.
- 2010 wurde 107 Mrd. E-Mails versendet (90 % SPAM).
- Wichtige Anhänge, die auch Benutzer bezogene Daten enthalten, werden arglos als Email versendet. (Kontonr, BLZ, PIN, Betrag, etc.)

Email und Verschlüsselung

- Beim Versand werden die Daten meist über SMTPS verschlüsselt zum Mailserver übertragen.
- Auch das Abholen der Mails erfolgt meistens über POP3S oder IMAPS Protokolle.
- Jedoch auf den Servern liegen die Mails – wenn nicht verschlüsselt – lesbar.
- Das gilt nicht nur für den Body der Mails, sondern auch für die **Anhänge**.

Email und Verschlüsselung

- Die meisten Angriffe gegen Unternehmen erfolgen von Innen.
- Welchen Weg eine Mail über das Internet geht und auf welchen dieser Server Mails gespeichert und mitgelesen werden ist nicht bekannt.
- Auf dem Weg zum Empfänger kann eine Mail auch verändert und deren Inhalt verfälscht werden.

Email und Verschlüsselung

- Alles gute Gründe E-Mails zu verschlüsseln.

  aber -

Warum macht das keiner ?

Gute Sicherung gegen Angriffe von aussen

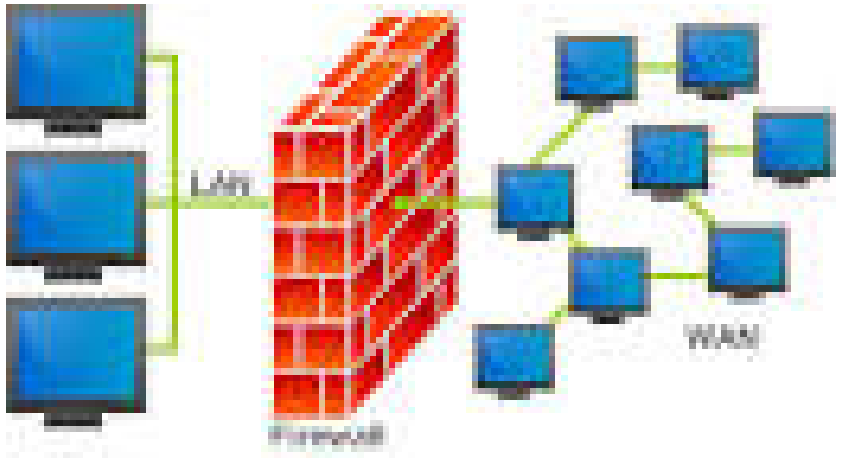
- Viele Firmen haben hervorragende Sicherheits-vorkehrungen gegen Angriffe von ausserhalb geschaffen.

- Wie sieht es aber mit der Sicherheit innerhalb eines LAN aus?

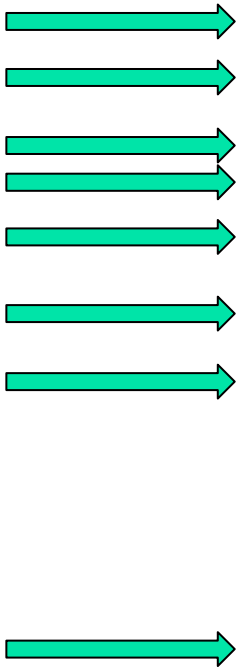
- Telnet, Ftp, Email Versand und Empfang sind selten geschützt.

Gute Sicherung gegen Angriffe von aussen

- Schutz gegen Angriffe von aussen.
- Nur authorisierte WAN Gäste haben Zugriff auf das interne Netzwerk.
- Wird über Firewalls, Router, VPN usw. realisiert.



Schwachstellen bei FTP



Follow TCP Stream

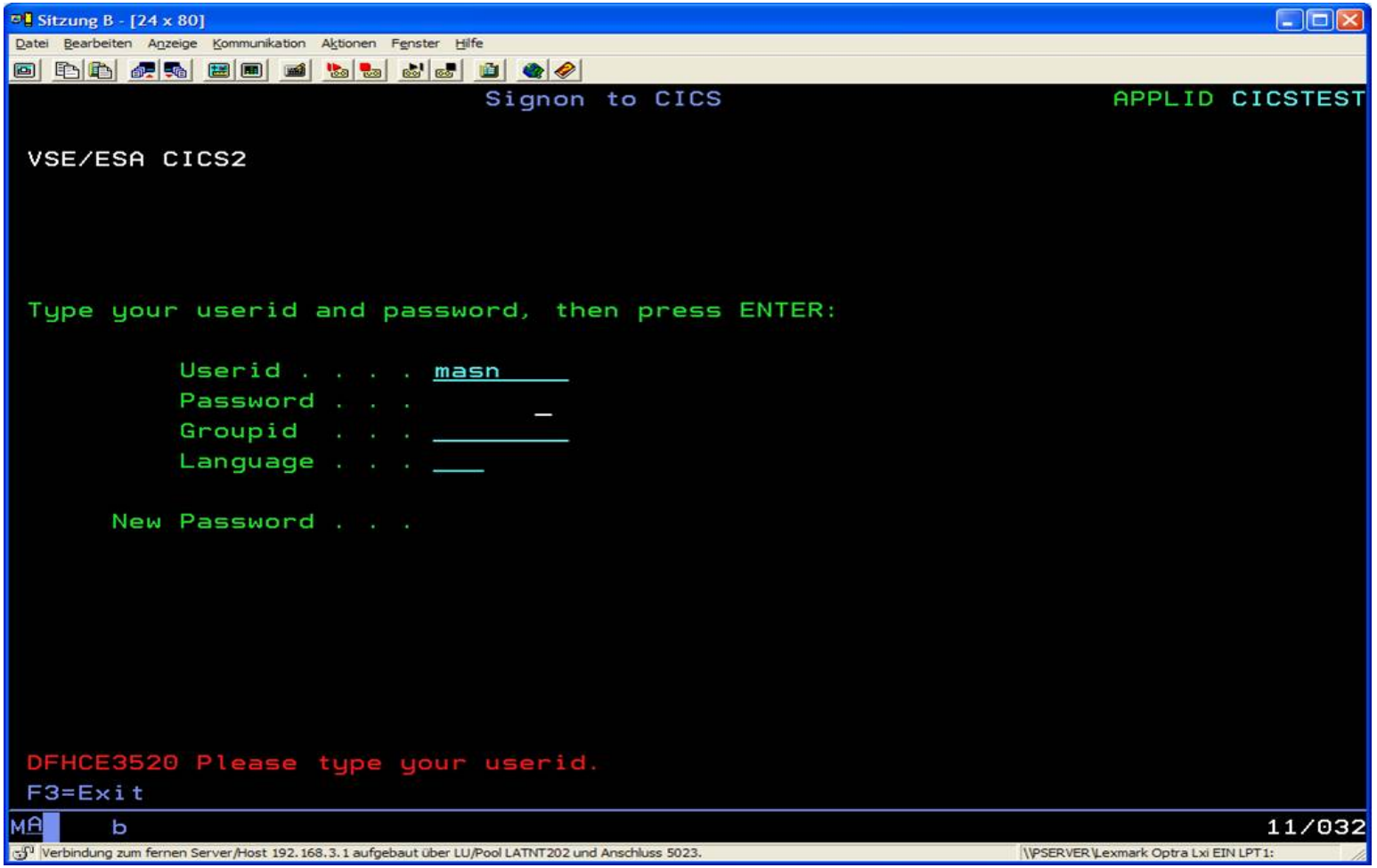
Stream Content

```
220-TCP/IP for VSE Internal FTPDAEMN 01.05 F 20090205 02.33
    Copyright (c) 1995,2006 Connectivity Systems Incorporated
220 Ready for new user
USER masn
331 User name okay, need password
PASS geheim
230 User logged in, proceed
PORT 192,168,197,40,65,55
200 Command okay
NLST
150 File status okay; about to open data connection
226 Closing data connection
CWD power.lst.l
250 Requested file action okay, completed
PORT 192,168,197,40,65,58
200 Command okay
RETR cpg
150-About to open active data connection
    File:POWER.LST.L.CPG
    Type:ASCII Recfm:V Lrecl:   256
    CC=ON UNIX=OFF RECLF=OFF TRCC=OFF CRLF=ON NAT=NO CONT=OFF
    Translate with US_ENG_03
    MODE=Stream  STRU=File
150 File status okay; about to open data connection
226-Bytes sent: 15,479
    Records sent: 184
    Transfer Seconds:          .22 (    69K per second)
    File I/O Seconds:          .01 (  1512K per second)
226 Closing data connection
QUIT
221 FTPDaemn closing control connection
```

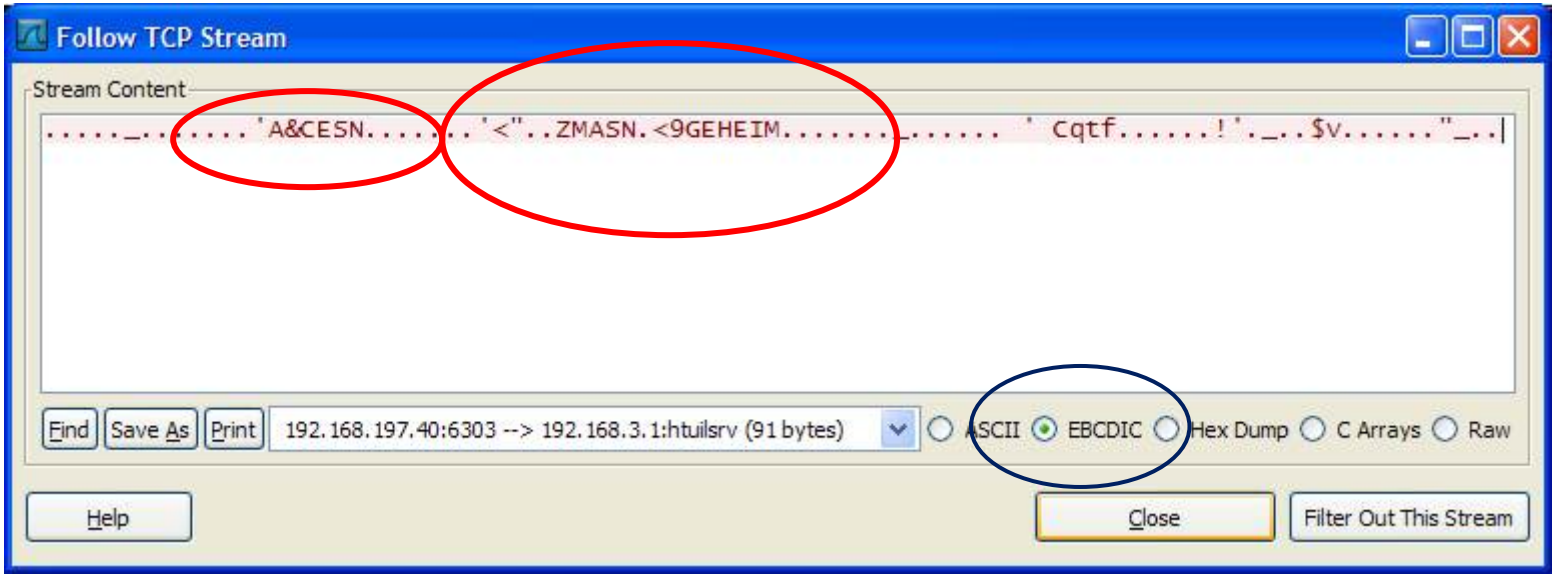
Find | Save As | Print | Entire conversation (1001 bytes) | ASCII | EBCDIC | Hex Dump | C Arrays | Raw

Help | Close | Filter Out This Stream

Schwachstellen bei Telnet



Schwachstellen bei Telnet



Kann sogar im Klartext mitgelesen werden !

Geht aber auch über Dumps, VTAM Trace, usw.

Schwachstellen bei Email

- Email Systeme können den Transfer mit SMTPS oder IMAPS verschlüseln.
- Besser sind jedoch eigene Verfahren wie PGP mit private und public Key.
- Anhänge, die kritische Daten beinhalten sollten auf jeden Fall verschlüsselt werden. (Nicht nur zippen!)

Telnet absichern

- Auch Telnet kann verschlüsselte Daten senden und empfangen.

- Telnet 3270 over SSL

- Ausführlich beschrieben:

ftp://public.dhe.ibm.com/eserver/zseries/zos/vse/pdf3/How_to_setup_Secure_Telnet_with_VSE.pdf

Secure FTP

- SecureFTP unterstützt User Authentication, privacy und Integrität mit Verwendung von RSA digital signierten Zertifikaten, DES Encryption und SHA-1 Secure Hash Funktionen

  - SecureFTP ist im TCP/IP for VSE ab z/VSE V4.1 und höher enthalten. (Ohne Zusatzkosten) oder als Zusatzoption kostenpflichtig von CSI!

- Ausführlich beschrieben:

ftp://ftp.software.ibm.com/eserver/zseries/zos/vse/pdf3/How_to_setup_SecureFTP_with_VSE.pdf

Haben Sie noch Fragen?

Themenvorschläge
für unsere nächste Tagung?

Vielen Dank

für Ihre Aufmerksamkeit !