CHECKLISTE FÜR UNIVERSAL-DILETTANTEN

LITTLE

CK OF ALL TRAD

WITH

SUITABLE REPRESENTATIONS

DIE VORTRAGENDEN

CHRISTOPH STOETTNER (STOEPS)

Macht seit 30 Jahren was mit Computern, erst mit Amiga 500, dann OS/2, Linux, ab und zu Windows, Mac OS X.

Linux und OSS seit den fruehen Anfängen (erstes Linux von einer Heft CD des DOS Magazins - 0.x)

Real nerds don’t click!

MARTIN LEYRER (DER LEYRER)

Der Leyrer arbeitet seit fast 40 Jahren mit Computern, seit 30 Jahren verdient er Geld damit.

Neben bzw. im Zuge seiner Tätigkeit als Senior Lab Services Consultant zerrt er Sysadmins aus den 1990ern ins 21. Jhdt.

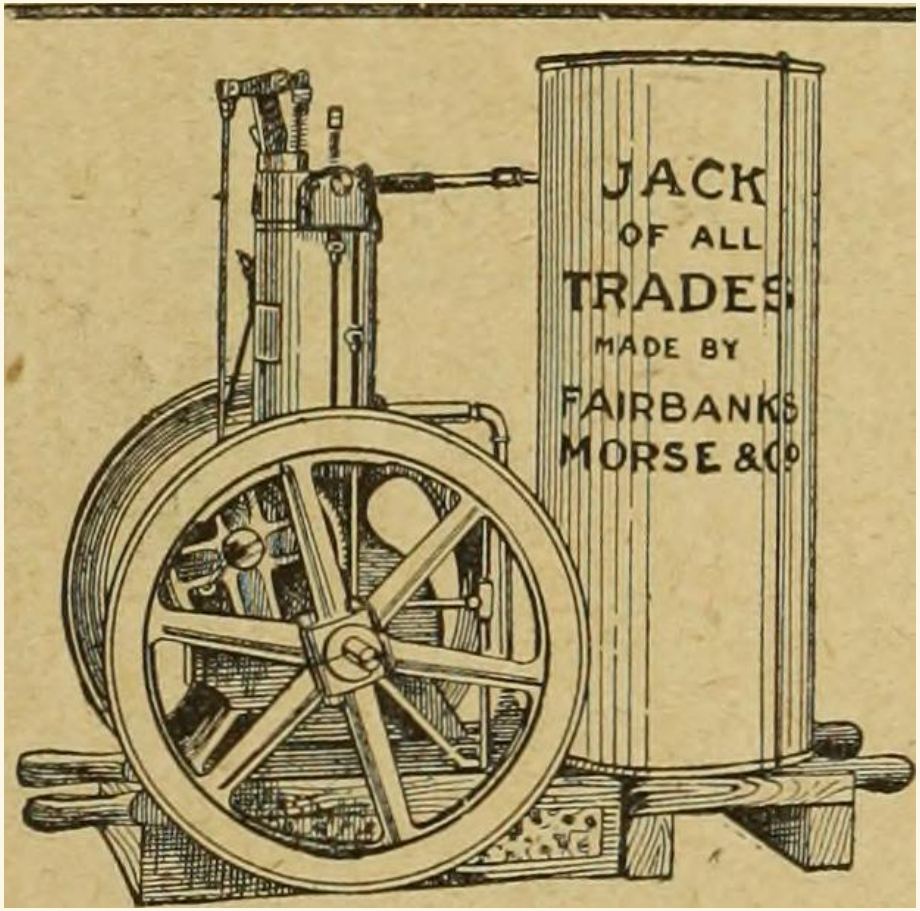
Darüber hinaus versucht er BesucherInnen diverser Veranstaltungen die Freuden der Linux Kommandozeile näher zu bringen.

(Immer noch auf der Suche nach einem NeXTcube).

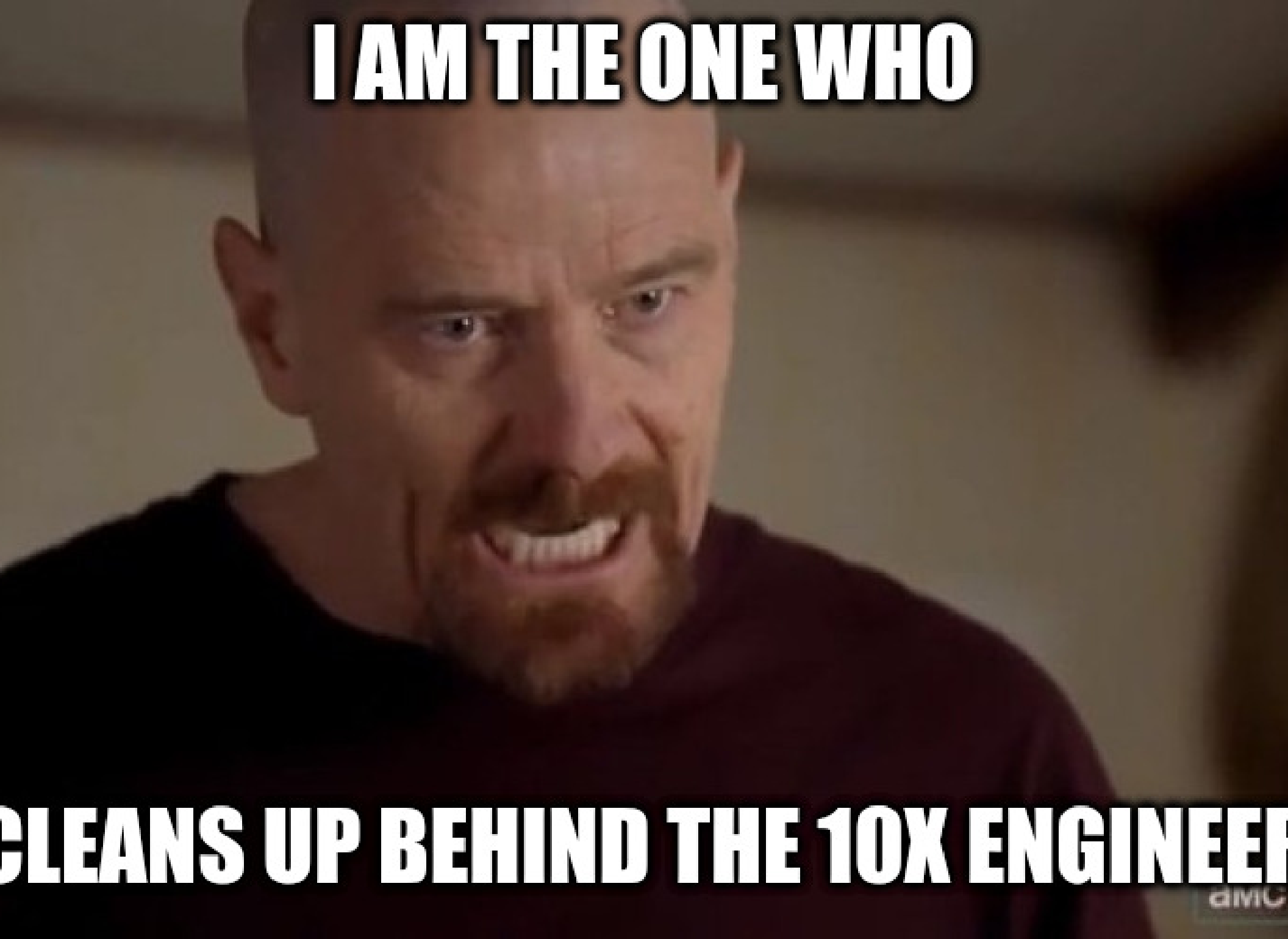
"T-SHAPED-PROFESSIONALS"

Der senkrechte Strich des T symbolisiert dabei das Spezialwissen, während der Querstrich das Breitenwissen darstellt.

DISCLAIMER



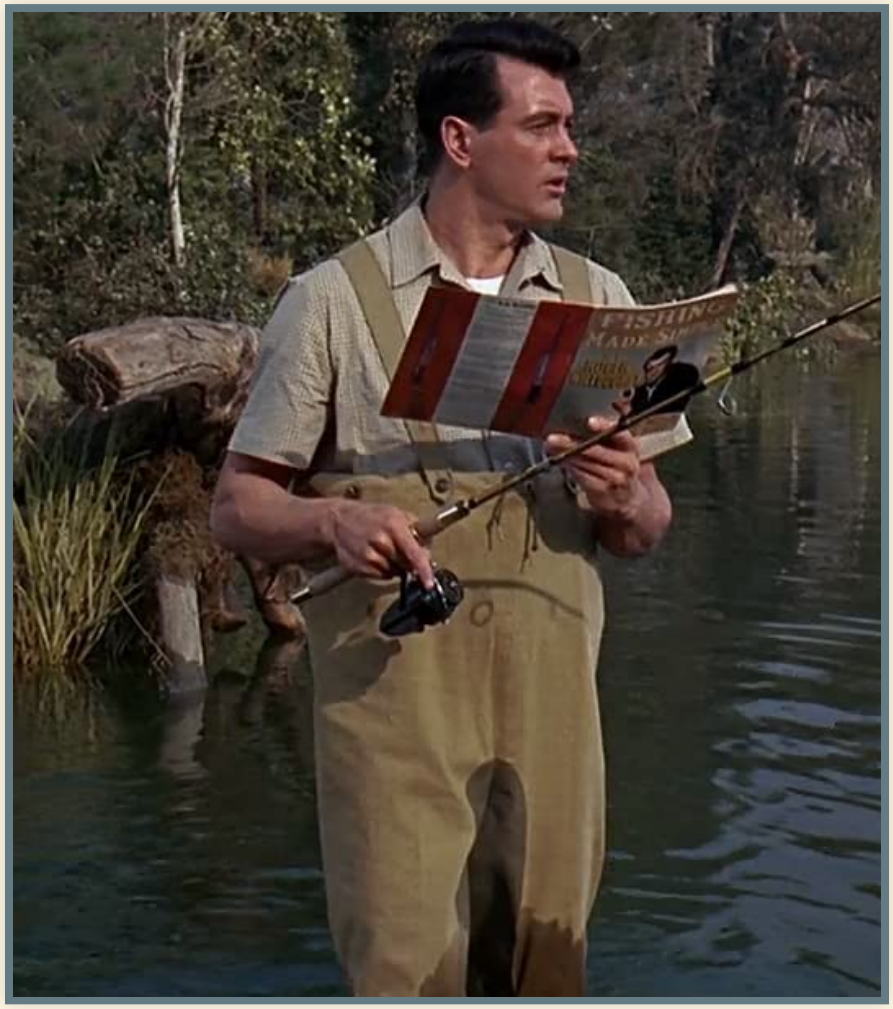
- Subjektiv
- Keinesfalls vollständig
- Keinesfalls ein Karrierevorschlag
- Denkanstoß
- YMMV
- ~~10x engineer~~


I AM THE ONE WHO
CLEANS UP BEHIND THE 10X ENGINEER

SOFT SKILLS

MAN'S FAVORITE SPORTS

- Erfolgreicher Angelgeräte-Verkäufer Roger Willoughby, der selbst nie angeln war
- Guter Zuhörer, gibt Tipps von einem Kunden an den Anderen weiter



DATENSAMMELLEITSCHIENE

- Lernt Englisch
- Lernt mehr Fremdsprachen
- Aber fangt mit Englisch an

WARUM ?

- Die meiste SW kommt nicht aus DACH
- Standards (RFCs, …) werden in Englisch verfasst
- "Bad English" ist die lingua franca in der IT
- Übersetzungen: spät und/oder in fragwürdiger Qualität
- Schnellere Round-Trips im Support

LERNT MEHR FREMDSPRACHEN

- Bash
- Python
- Perl
- PowerShell
- Javascript
- …

WISSENSTIEFE

Man sollte mind. soviel wissen, dass man eine Installation kaputt und wieder heile machen kann.

DIPLOMATIE / SELBSTBEWUSSTSEIN

- "Das haben wir schon immer so gemacht."
- "Kann man schon so machen, ist dann halt Kacke"
- Soll es funktionieren, oder so sein wie Sales es verkauft hat

NEIN SAGEN

- It is required to manually [via JS, Anm.] encrypt the password to prevent from data stealing by the adversary if in case man in the middle attack is accomplished.
- NEIN! (Ja, Du musst alles Beweisen)

EXCEL

- Je grösser ein Unternehmen desto öfter trifft man auf Excel für [1]
  - Dokumentation
  - Projektmanagement

DOKUMENTATION / TECHNICAL WRITING

- Wer schreibt bleibt
- Nur Text Formate erleichtern die Erfassung
  - Markdown / mkdocs
  - Asciidoc(tor)
- Konvertierung in Zielformate pdf, word, LaTeX über `pandoc`
- Öffentlich (Karriere?)

CYAM - COVER YOUR ASS MAILS

- Moscow rules: watch your back
- London rules: cover your arse
- Für die "told you so" Momente

FRAGEN UND ANWORTEN

Nein, wir sind noch nicht bei der Q&A angelangt, keine Panik.

WARUM IST DAS WICHTIG?

- Junior "nervt" Senior
- Support liefert keine Antworten
- Kundentickets mit "XYZ funktioniert nicht"

FRAGEN "RICHTIG" STELLEN [1]

- Verwende aussagekräftige, genaue Betreffzeilen
- Sei genau und informativ bei der Beschreibung deines Problems
- Beschreibe das Ziel, nicht einen Schritt
- Stelle eine deutliche Frage
- Poste die Lösung

---

1. https://tty1.net/smart-questions_de.html

FRAGEN UMDREHEN

- WAS wollen Sie eigentlich erreichen?
- Welche Schritte haben Sie durchgeführt?
- Welche konkrete Fehlermeldung wird angezeigt?
- Welche Version von OS, Produkt XYZ, …?
- usw.

RUBBERDUCKING

Beim Quietscheentchen-Debugging[1] wird das aktuelle Problem detailliert ("Zeile für Zeile") einem Quietscheentchen erklärt.

Während des Erklärungsprozesses fällt dir oft der Fehler auf. Der Vorteil des Quietscheentchens gegenüber einer anderen Person ist, dass niemand gestört werden muss.

---

1. "The Pragmatic Programmer: From Journeyman to Master", Andrew Hunt and David Thomas (ISBN 978-0135957059)

HARD SKILLS

LERNT GOOGLE ZU BEDIENEN

- "Wissen heißt wissen, wo es geschrieben steht" — Alber Einstein
- https://support.google.com/websearch/answer/246643 hl=en
- Stack Overflow, Server Fault, Super User, … haben eine Suche
- Microsoft hat suchbare "Doku"
- man pages sind Dein Freund

LOGS SIND DEINE FREUNDE

ENGLISCHE LOGS !!!111ELF111!!!!

```
[21.01.22 05:08:20:905 MEZ] 000000ad SchedulerServ E   SCHD0128E:
Der D?mon f?r den Scheduler scheduler/metrics konnte nicht
gestartet werden:
com.ibm.ws.scheduler.exception.SchedulerDataStoreException:
SCHD0124E: scheduler/metrics kann nicht initialisiert werden
```

LERNT LOGS LESEN

Spoiler: Wenn Ihr logs lesen, die Fehlermeldung/code goggeln und dann 1-2 Lösungsansätze ausprobieren könnt, seit ihr meist schon die Heroes.

Ja, es IST oft so trivial.

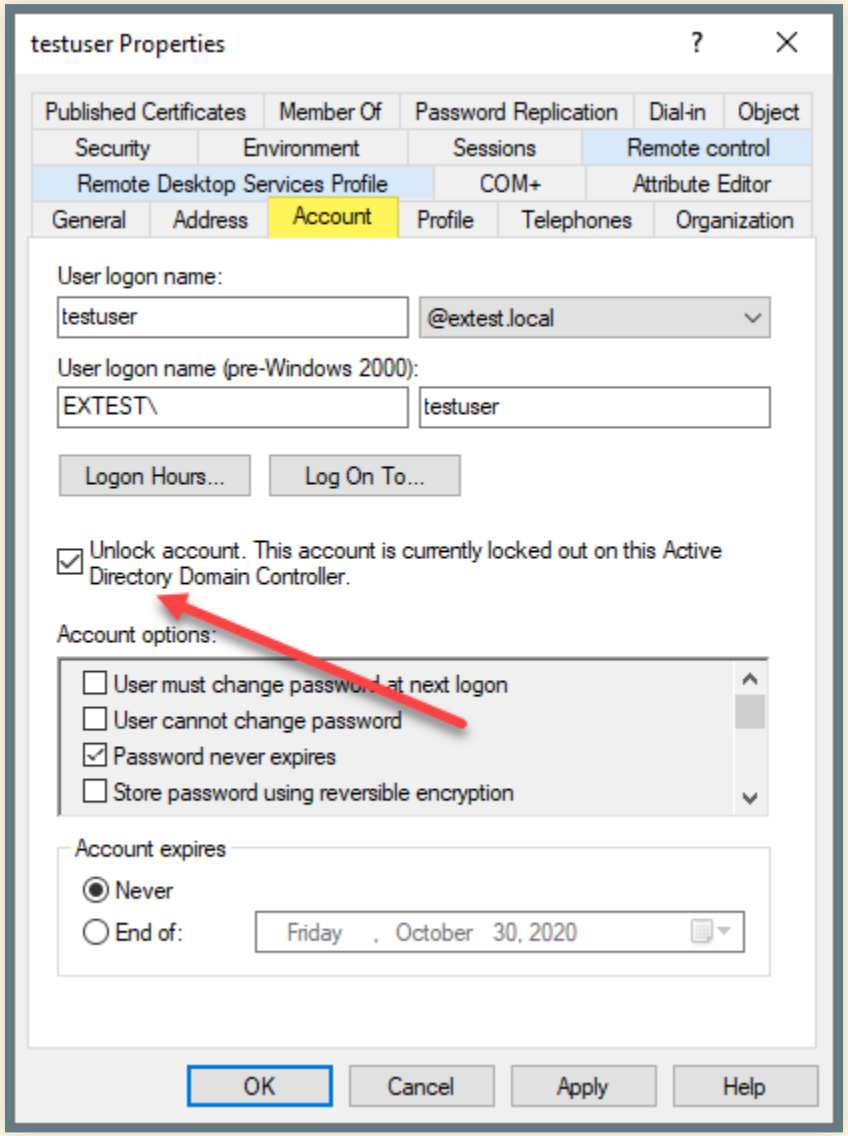
BEISPIEL 0

```
com.ibm.websphere.wim.exception.PasswordCheckFailedException: CWW
The password verification for the 'binduser' principal name faile
Root cause: 'javax.naming.AuthenticationException:
[LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9,
comment: AcceptSecurityContext error, data 52e, v1db1]
```

BEISPIEL 1

```
com.ibm.websphere.wim.exception.PasswordCheckFailedException: CWW
The password verification for the 'binduser' principal name faile
Root cause: 'javax.naming.AuthenticationException:
[LDAP: error code 49 - 80090308: LdapErr: DSID-0C0903A9,
comment: AcceptSecurityContext error, data 775, v1db1]
```

LÖSUNG – JA, DU MUSST ALLES BEWEISEN



STORAGE 1/2

- NFS
- CIFS
- EC2, cephfs, glusterfs, …
- "Spindeln", HABs, LUNs, shared NICs, ….
- disk i/o vs. eg. Windows "Avg. Disk Queue Length"

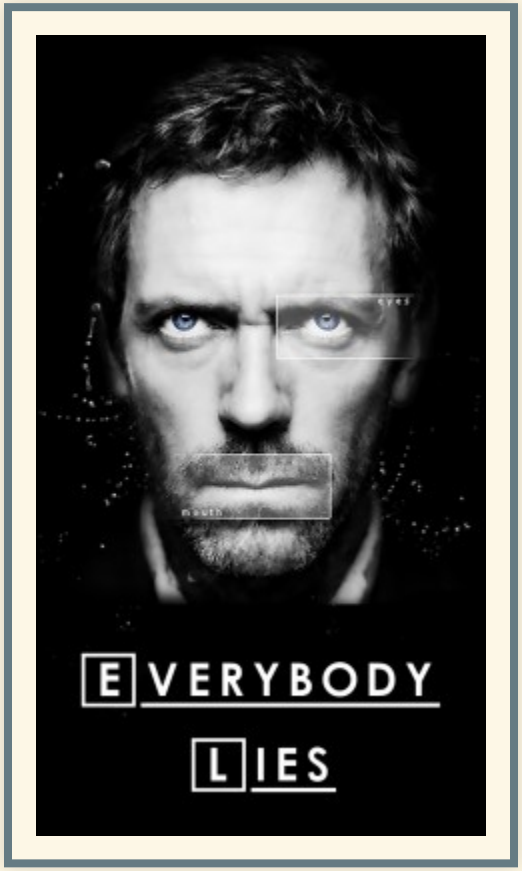
STORAGE 2/2

- Die Storage Admins sagen immer dass der Storage schnell und nicht Schuld an Problemen ist.
- Ja, ihr müsst immer das Gegenteil beweisen.

NETZWERK

- It’s always DNS
- It’s always the cable/switch port
- Liebet und ehret das hosts file, ausser ihr arbeitet mit K8s
- Wenn ein Kunde von "WINS" statt DNS spricht, lauft!

NETZWERKSICHERHEIT



- Alle Ports sind offen
- Da ist keine WAF oder Reverse Proxy dazwischen
- Admins: das Netzwerk ist schnell und nicht Schuld an Problemen
- Ja, Ihr müsst immer das Gegenteil beweisen

PCAP OR IT DIDN'T HAPPEN

- Wireshark ist Dein Freund
- pcaps sammeln und analysieren
- Übung macht den Meister
- Schon mal TLS mitgelesen?

ZERTIFIKATE

- CAs, certificate chains
- cer, crt, pem, p12, pfx, …
- openssl zum konvertieren
- openssl s_client zum Testen
- `testssl.sh` und https://keystore-explorer.org ersparen das Googlen von openssl commands
- CRLs und Online Certificate Status Protocol (OCSP)

WEBSERVERZERTIFIKAT

Welche Files brauch ich, um TLS bei einem Webserver einzurichten?

- public server certificate
- PRIVATE KEY
- intermediate certificates
- root certificate
- Reihenfolge!

ZERTIFIKAT ABGELAUFEN

- Kalendereintrag
- Monitoring
- cerbot (BITTE!!!!)
- Welcher Zertstore

DOMAIN REGISTRIERUNG NICHT ERNEUERT

- An sich auch nur DNS
- 30 Tage Uebergangsfrist, muss jährlich erneuert werden

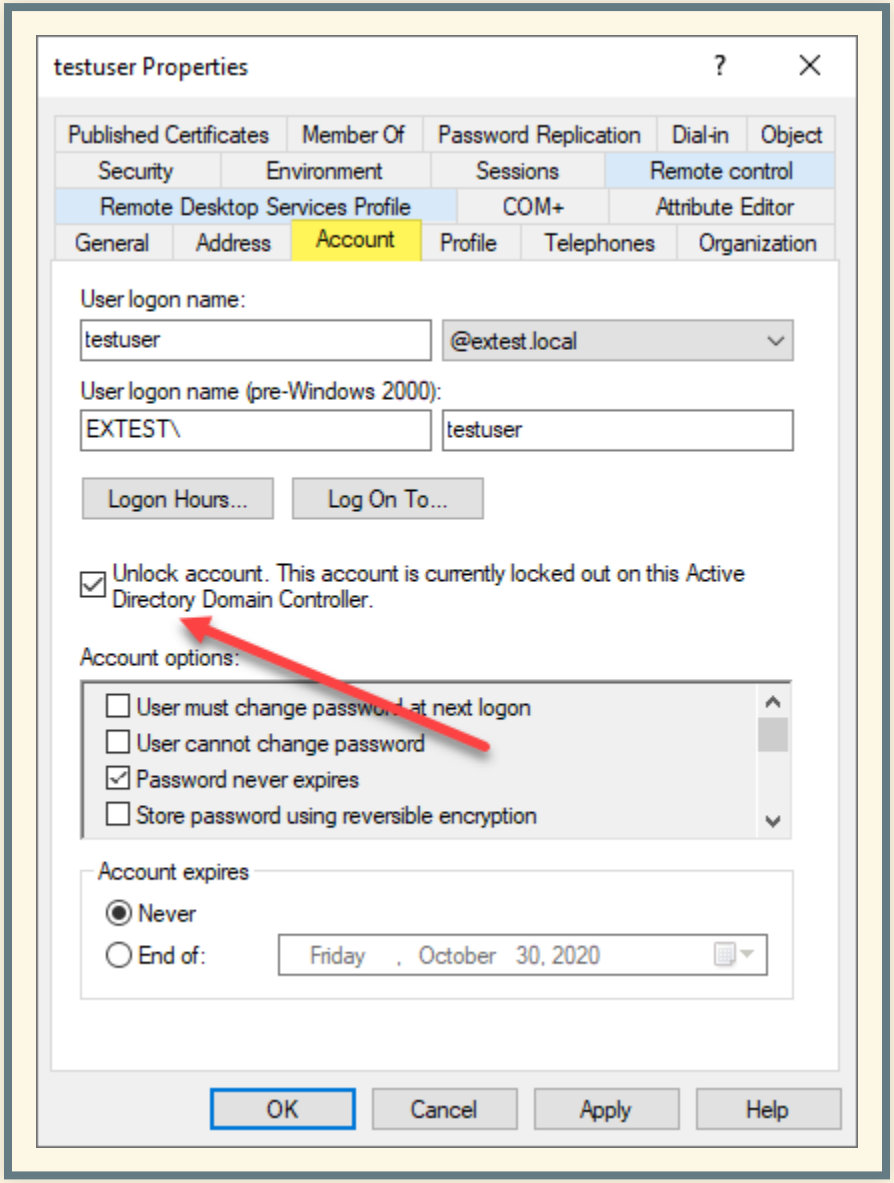
HTTP BASICS

- http solltet Ihr verstehen
- http header und cookies, Gültigkeitsbereich, …
- http error codes
- Gilt analog für SIP, WSS, …

HTTP TOOLS

- MEHRERE Browser (P… Mode!)
- Browser Developer Tools
- Fiddler, Burp suite und Co. (MITM)
- har files lesen - understand the flow
- Antwortet die Firewall, WAF, reverse proxy oder app server
- Ja, ihr müsst beweisen, wer den HTTP 500 sendet

AUTHENTIFIZIERUNG & SSO



- LDAP
- AD
- SAML / OAuth / OpenID Connect
- Fehlermeldungen verstehen

SINGLE SIGN ON

- SAML
- OAuth / OpenID Connect
- SPNEGO / Kerberos
- Grundlagen, Logging and Tracing
- Grundlegende Einstellungen
  - am Besten mit Screenshots zum Vergleich

GRUNDLAGEN MOBILE DEVICES

- z.B. Zugriff auf Keystore nur fuer System Apps (iOS)
  - App hinter Azure Auth mit Device Zertifikat
- MDM
- VPN / Proxy / SSL Endpoints / MitM

TROUBLESHOOTING AUCH OHNE `root`

- `root` Rechte oft eingeschränkt
- `sudo -l` zeigt sudo Kommandos fuer den angemeldeten Benutzer
- pcap ohne root nicht möglich
- `telnet`, `netcat` zum Testen offener Ports

GTFOBINS

- Must read: https://gtfobins.github.io/
  - als Admin um den Zugriff zu verhindern
  - als User um sich einen Jira Task zu ersparen

GTFOBINS BEISPIEL

- Kurzes Beispiel [1]
- `docker`

root shell mit Berechtigung ueber Gruppe

```
docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

root shell per `sudo`

```
sudo docker run -v /:/mnt --rm -it alpine chroot /mnt sh
```

---

1. https://gtfobins.github.io/gtfobins/docker/

PORTABLE APPS

- Wenn der USB Port noch offen ist
- Du zumindest SW runterladen kannst
- Du Schreibrechte auf ein Dir hast
- https://portableapps.com/

AUGEN AUF - RSS ABO

- CVE eurer Hautpapplikationen
- OWASP Top 10
- Aktuelle Angriffe und deren Verteidigung
- Zero Days

WAS HAT SICH DIE LETZTEN JAHRE GEÄNDERT?

ERHÖHTE ABHÄNGIGKEITEN

- Höherer Zeitaufwand
- Anforderung an regelmässige Releasezyklen
  - z.B. DB wird auf aktuellste Version gepatcht
  - u.U. muss die eigene Applikation aktualisiert werden um diese Version zu unterstuetzen
- Erschwerte Fehlersuche
  - da nur noch Benutzerrechte
- Zentrales Logging kann hier helfen

JENSEITS DES TELLERRANDS

- Du bist nicht "nur" $Produkt/$Technologie-Admin
- Holistischer Zugang (DevSec*Ops)
- Business Needs

Milestones in the Technology Industry

CES® Celebrates 50 Years of Innovation

1968
The computer mouse is demonstrated by Douglas Engebart, commercialized by the Apple Macintosh 16 years later.

1971
Electronic tuning is first seen in U.S. TVs.

1972
The first home videogames, designed to play through TV receivers, are marketed.

1976
The first microprocessor videogames are marketed.

CES 1975
The first VHS VCR is introduced at CES.

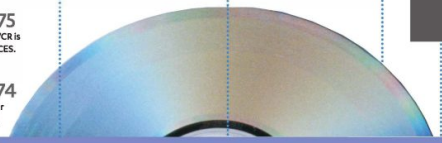
CES 1974
Laserdisc Player debuts at CES.

1978
CES is held in Las Vegas for the first time.

1977
Apple Computer Inc. introduces its first personal computer.

1982
Dolby Laboratories introduces surround sound for home use.

1982
The first compact disc (CD) players go on sale in the United States.



1985
The CD-Rom is introduced.

1992
The MiniDisc makes its debut.

1994
The first CES Mexico is held in Mexico City

CES 1994
First public demonstration of DSS (Digital Satellite System) receiver at CES.

1994
GPS auto navigation systems are marketed in the United States.

1998
CD-Recordable decks are first sold.

1998
E-Commerce takes off, with as many as 30 million U.S. households purchasing products over the internet in 1998.

1998
Diamond Multimedia introduces the first portable MP3 device.

CES 2001
Internet gaming is introduced by Microsoft and Sony at CES.

2001
Satellite radio broadcasting begins.

2001
First high-speed, next-generation cell phone networks are activated.

2003
First HDTV camcorders enter the marketplace.

2003
FCC approves cable-CE "plug-and-play" agreement.

CES 2003
Blu-ray DVD and HDTV DVR debut at CES

2005
First hard disk drive-based camcorders go on sale.

2005
First HDTV with built-in HD-DVR goes on sale.

2005
IPTV

2007
CES celebrates its 40th anniversary.

2007
Convergence of Content & Tech

2007
Apple introduces its iPhone.

CES 2009
3D HDTV debuts at CES.

CES 2011
Connected TVs, Smart Appliances, Android Honeycomb, Ford's Electric Focus, Motorola Atrix, Microsoft Avatar Kinect all introduced at CES.

2015
In step with tech evolution, CEA becomes the Consumer Technology Association.

2015
First 4K Ultra HD Blu-ray decks go on sale.

2015
Apple starts selling the Apple Watch.

1967 | 1975 | 1980 | 1985 | 1995 | 2000 | 2004 | 2007 | 2011 | 2017

1969
ARPANET, a forerunner of the internet, becomes operational.

1973
The first Winter Consumer Electronics Show (CES) is held in Chicago.

1970
The computer floppy disk is developed.

1970
Intel introduces the computer memory chip.

1970
Videocassette Recorder (VCR) debuts at CES.

1967
The first Consumer Electronics Show is held in New York City.

1975
The first personal computer, Altair 8800 debuts.

1975
The first Betamax VCR is introduced.

1975
CB radio becomes a major consumer product.

1975
The laser printer is introduced.

1975
The first liquid crystal displays (LCD) are sold.

1981
IBM PC, using Microsoft's Disk Operating System (MS-DOS), is introduced.

1980
The first portable VCR-camera combinations (camcorders) are demonstrated.

1979
Personal headset audio is introduced.

1984
Sales of stereo color TV receivers and adapters begin.

1984
EIA's Consumer Electronics Group champions the Supreme Court's Betamax decision to allow consumers to record TV programs for their own personal use.

1983
Apple's Lisa, the first computer using a graphical user interface (GUI) and mouse, is unveiled.

1983
Cellular telephone service is introduced.

1991
Multimedia CD-ROM computer systems are introduced.

1993
Personal Digital Assistants (PDA) are introduced.

1987
The movie theater experience moves into the living room: Dolby Pro Logic is available at home.

1997
DVD players debut in the United States.

1996
Set-top boxes plug into televisions and allow viewers to surf the internet's World Wide Web via remote control.

1996
Congress passes the Telecommunications Act of 1996.

1998
The first HDTV sets are sold at retail.

1995
Flat-screen plasma display TVs are introduced.

1995
EIA's Consumer Electronics Group becomes the Consumer Electronics Manufacturers Association (CEMA).

2000
First Bluetooth-enabled products are launched.

2000
Secure, high-capacity, solid-state flash media formats and products are introduced.

CES 2000
An HDTV-DVD player is demonstrated at CES.

2000
CEMA becomes its own corporate entity and renames itself the Consumer Electronics Association (CEA).

1999
Hard disk-based digital personal video recorders (PVRs) are first introduced at CES, capable of "smart" programming and instantaneous playback of a recorded TV program, even while the program is running.

1999
DVD-Audio and Super Audio CD (SACD) players are introduced.

1999
The first high-definition plasma display screen is introduced at CES.

2002
First combination cell phones/digital cameras become available.

2002
Blu-ray and red laser high-definition DVD recording standards are announced.

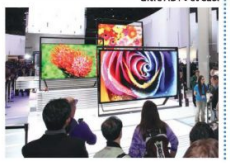
2004
HD Radio

2004
First U.S. 3G cellular network service and phones announced.

2004
Annual sales of U.S. consumer electronics surpass $100 billion.

2004
Combination cable HDTV STB and HDTV PVRs and Cable-CARD- equipped DTVs go on sale.

2004
SINOCES debuts



2012
3D Printers

2006
First videogame systems with high-definition DVD players hit the market.

CES 2012
Ultrabooks, 3D OLED, Android 4.0 tablets all introduced at CES

2012
3D OLED

2012
Android 4.0 Tablets

2006
First 1080p plasma HDTVs are introduced.

2012
CES Asia launches

2013
Ultra HDTV at CES.

2016
First 4K Ultra HD Blu-ray decks and UHD Blu-ray Discs go on sale

2016
FCC votes to "unlock" cable set-top box converters

2014
Digital cameras and smartphones with 4K video recording capabilities go on sale.

2014
3D Printers, Curved UHD and wearable technologies are shown at CES

2013
GoPro, maker of action camcorders, becomes leading camcorder seller in U.S.

2017
Celebrating 50 Years
CES | 1967-2017

Consumer Technology Association™

Celebrating 50 YEARS
CES | 1967-2017

FRAGEN?

- STOEPS
  - @stoeps
  - https://stoeps.de/
- LEYRER
  - @leyrer
  - https://martin.leyrer.priv.at/