Einen sicheren Laptop mit Ubuntu einrichten

Stefan Schumacher

sicherheitsforschung-magdeburg.de
stefan.schumacher@sicherheitsforschung-magdeburg.de

Chemnitzer Linux-Tage

Über Mich

Über Mich

- Geek, Nerd, Hacker seit knapp 20 Jahren
- Berater für Finanzinstitute, Regierungen, Sicherheitsbehörden
- Direktor des Magdeburger Instituts für Sicherheitsforschung
  Forschungsprogramme zur Unternehmenssicherheit
- Herausgeber des Magdeburger Journals zur Sicherheitsforschung
- `www.Sicherheitsforschung-Magdeburg.de`

Inhaltsverzeichnis

Bedrohungslage

- Schadsoftware greift Rechner an
- mobile Rechner gehen verloren oder werden gestohlen
- Manipulationen einfach möglich bei physischer Kontrolle
- Daten abschöpfen im Hotel
- Trojaner aufspielen bei »Zollkontrolle«
- sensible Daten schützen

Warum Linux?

- kostenlos, frei, offen
- Open Source - Backdoors verstecken schwierig
- Unix-Sicherheitsmodell
- gute Hardwareunterstützung
- vielfältige Software verfügbar

Warum Ubuntu?

- Ubuntu recht einfach nutzbar
- unterstützt von Canonical
- viele Anwendungen verfügbar
- 2 Releases pro Jahr (.04 und .10)
- LTS mit 5 Jahren Laufzeit (18.04., 16.04., 14.04, 12.04)
- Alternate Install/Server existiert

Bedrohungsszenario

- Abwägung Aufwand und Kosten vs. Bedrohung und Sicherheit
- Was bedroht mich?
- Risikoanalyse!
- Grundlage der Journalistenschulung für Syrien

Inhaltsverzeichnis

Hardware

- professionelle Laptops mit ordentlichem BIOS/UEFI
- Lenovo Thinkpad, Dell Latitude, HP Elitebook
- Thinkpad-BIOS besonders geschützt
- BIOS: User, Admin und Festplattenpasswort setzen
- gebrauchten Wegwerflaptop/Netbook
- z.B. Lapstore
- Hardwaremanipulationen existieren - Rechner nicht aus den Augen lassen

Hardware

- SSD: Samsung 850 Pro 1TB
- SSD: Samsung 850 Evo 1TB
- Hardwareverschlüsselung in AES
- immer aktiviert
- Festplattenpasswort im BIOS setzen
- cf: OPAL TCG
- Sicherheitsprobleme! (cf. Self-encrypting deception: weaknesses in the encryption of solid state drives (SSDs) by Meijer and Gastel)

Hardware

Inhaltsverzeichnis

VERSCHLÜSSELUNG

- Verschlüsselung der gesamten Festplatte (LVM LUKS)
- Verschlüsselung von user durch ecryptfs (deprecated)
- Verschlüsselung beliebiger Verzeichnisse durch gocryptfs/cryfs/encfs
- Verschlüsselung einzelner Dateien durch mcrypt, OpenSSL oder GnuPG
- sicheres Passwort!
  min. 12 Zeichen, Groß/Kleinbuchstaben, Ziffern, Sonderzeichen, keine Wörter aus dem Wörterbuch

VERSCHLÜSSELUNG

- Verschlüsselung der gesamten Festplatte (LVM LUKS)
- Verschlüsselung von user durch ecryptfs (deprecated)
- Verschlüsselung beliebiger Verzeichnisse durch gocryptfs/cryfs/encfs
- Verschlüsselung einzelner Dateien durch mcrypt, OpenSSL oder GnuPG
- sicheres Passwort!
  min. 12 Zeichen, Groß/Kleinbuchstaben, Ziffern, Sonderzeichen, keine Wörter aus dem Wörterbuch

Passwörter

- werden gehasht gespeichert
- Hash := mathematische Einwegfunktion
- Passwort $\rightsquigarrow$ Hash: einfach
- Hash $\rightsquigarrow$ Passwort: schwer

Magdeburg	`59aceadf846f772736c4b40eee7b155d`
magdeburg	`7712722364ae231b5f777bac5dd2eb80`
MagdeBurg	`eadfc761160224295a58847eee4cbdfc`
Magdeburger	`0c52463fc68f157a5756cdde4adf762d`
Magdeburgerin	`68a783bebaf27a448481d5341b77b4f9`

Wörterbuchangriffe

fröhliches Passwortraten: alle Kombinationen probieren

Kombinationen = Alphabet ^ Länge

$10^3 = 1.000$

Wörterbuchangriffe

fröhliches Passwortraten: alle Kombinationen probieren

Kombinationen = Alphabet ^ Länge

$10^3 = 1.000$

26 Buchstaben (a-z), 5 Stellen: $26^5 = 11.881.376$

```
aaaaa  aaaba  aaaca  ...  zzzya  zzzza
aaaab  aaabb  aaacb  ...  zzzyb  zzzzb
aaaac  aaabc  aaacc  ...  zzzyc  zzzzc
aaaad  aaabd  aaacd  ...  zzzyd  zzzzd
aaaae  aaabe  aaace  ...  zzzye  zzzze
                     ...
aaaav  aaabv  aaacv  ...  zzzyv  zzzzv
aaaaw  aaabw  aaacw  ...  zzzyw  zzzzw
aaaax  aaabx  aaacx  ...  zzzyx  zzzzx
aaaay  aaaby  aaacy  ...  zzzyy  zzzzy
aaaaz  aaabz  aaacz  ...  zzzyz  zzzzz
```

Wörterbuchangriffe

Kombinatorik

- $99^{10} = 90.438.207.500.880.449.001$ (Trillionen)
- $99^{15} = 860.058.354.641.288.524.893.953.951.499$ (Quadrilliarden)
- $99^{20} = 8.179.069.375.972.308.708.891.986.605.443.361.898.001$ (Sextilliarden)
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365.000 \approx 570$ Millionen Jahrtausende

Wörterbuchangriffe

Kombinatorik

- $99^{10} = 90.438.207.500.880.449.001$ (Trillionen)
- $99^{15} = 860.058.354.641.288.524.893.953.951.499$ (Quadrilliarden)
- $99^{20} = 8.179.069.375.972.308.708.891.986.605.443.361.898.001$ (Sextilliarden)
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365.000 \approx 570$ Millionen Jahrtausende
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40\ Minuten$
- $(99^{10}/432.000.000)/365.000 \approx 570$ Tausend Jahrtausende
- $(99^{20}) = 51.871.317.706.572.226.717.985.709$ Jahrtausende

Wörterbuchangriffe

Kombinatorik

- $99^{10} = 90.438.207.500.880.449.001$ (Trillionen)
- $99^{15} = 860.058.354.641.288.524.893.953.951.499$ (Quadrilliarden)
- $99^{20} = 8.179.069.375.972.308.708.891.986.605.443.361.898.001$ (Sextilliarden)
- Annahme: 5 Passwörter pro Sekunde $\rightsquigarrow$ 432000 pro Tag
- $\frac{26^5}{432.000} = 27,5$ Tage
- $(99^{10}/432.000)/365.000 \approx 570$ Millionen Jahrtausende
- Annahme: 5.000 Passwörter pro Sekunde $\rightsquigarrow$ 432.000.000 pro Tag
- $\frac{26^5}{432.000.000} \approx 40\ Minuten$
- $(99^{10}/432.000.000)/365.000 \approx 570$ Tausend Jahrtausende
- $(99^{20}) = 51.871.317.706.572.226.717.985.709$ Jahrtausende

Stratfor-Demo

- Stratfor-Demo

Wörterbuchangriffe

- Thomas Roth, 2010
- lässt alle 1-6 stelligen Passwörter generieren
- SHA-1 Hashes berechnen
- nutzt Amazon Cloud GPU Programm
- Dauer: 49 Minuten, Kosten 2,1$/h

Passwörter raten

- beliebte Social-Engineering-Methode
- Passwortwahl sagt einiges über den Benutzer aus
- muss einfach merkbar sein $\rightsquigarrow$ naheliegendes Datum
- Name des Sohnes/Tochter/Ehemann/Hund/Katze/Maus ...
- Postleitzahl, KFZ-Kennzeichen, Hochzeitstag, Geburtstag
- leicht herausfindbar (Pers-Akte, Lohnsteuerkarte, Blog, Homepage)
- Daher absolut verboten!

Passwörter raten

- beliebte Social-Engineering-Methode
- Passwortwahl sagt einiges über den Benutzer aus
- muss einfach merkbar sein $\rightsquigarrow$ naheliegendes Datum
- Name des Sohnes/Tochter/Ehemann/Hund/Katze/Maus ...
- Postleitzahl, KFZ-Kennzeichen, Hochzeitstag, Geburtstag
- leicht herausfindbar (Pers-Akte, Lohnsteuerkarte, Blog, Homepage)
- Daher absolut verboten!

Passwörter recyclen?

- mehrere Passwörter nötig $\rightsquigarrow$ Recycling
- Webforen etc. werden oft angegriffen
- Ist das Webforum vertrauenswürdig?
- Technisch einwandfrei? Oder gar Honeypot?

Auf keinen Fall überall das selbe Passwort verwenden!

Passwörter recyclen?

- mehrere Passwörter nötig $\rightsquigarrow$ Recycling
- Webforen etc. werden oft angegriffen
- Ist das Webforum vertrauenswürdig?
- Technisch einwandfrei? Oder gar Honeypot?

Auf keinen Fall überall das selbe Passwort verwenden!

Passwortregeln

- Verwenden Sie kein Passwort das erraten werden kann!
- Verwenden Sie kein Passwort das in einem Wörterbuch steht!
- Verwenden Sie ein langes Passwort mit Groß- und Kleinschreibung, Zahlen und Sonderzeichen!
- Das Passwort muss geheim bleiben!
- Verwenden Sie nicht überall das selbe Passwort!
- Wechseln Sie Ihre Passwörter!

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ W d g W g , E F F z s . - F S , 1 8 0 5

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- $\rightsquigarrow$ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen
- Wörter: LilaDederonKittelschürzeSchattenmorellenZuckerkuchen

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen
- Wörter: LilaDederonKittelschürzeSchattenmorellenZuckerkuchen
- 1920Mainz1923Quedlinburg1931Stralsund1935Rostock

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen
- Wörter: LilaDederonKittelschürzeSchattenmorellenZuckerkuchen
- 1920Mainz1923Quedlinburg1931Stralsund1935Rostock
- Passwortflyer

Passwörter von Hand generieren

- Einen Satz ausdenken und die Initialen zusammenziehen
- Wem der große Wurf gelungen ,
  Eines Freundes Freund zu sein.
  - Friedrich Schiller, 1805
- ⇝ W d g W g , E F F z s . - F S , 1 8 0 5
- Leetspeak: `D03s Any1 in |-|3r3 5pE4|< 31337?`
- Dialekte: Vocheljesank in Machteburch;
  Motschekiebschen
- Wörter: LilaDederonKittelschürzeSchattenmorellenZuckerkuchen
- 1920Mainz1923Quedlinburg1931Stralsund1935Rostock
- Passwortflyer

VERSCHLÜSSELUNG

- `Geführt - gesamte Platte mit verschlüsseltem LVM`
- `Manuell`
- `http://wiki.ubuntuusers.de/System_verschlüsseln/Alternate_Installation`
- `/` kann kaum mehr manipuliert werden, `/boot` schon
- `/boot` auf USB-Stick verschieben
- kann auch für USB-Sticks oder USB-Platten eingesetzt

VERSCHLÜSSELUNG

- eCryptFS: verschlüsselt das Benutzerverzeichnis (`/home/stefan/`) (deprecated)
- verschlüsselt im Dateisystem, Passwort automatisch aus User-Passwort abgeleitet
- wird automatisch bei der Installation mit eingerichtet
- Nutzung transparent
- schützt aber nur Nutzerdateien, nicht Systemdateien

VERSCHLÜSSELUNG

- encfs: verschlüsselt ein beliebiges Verzeichnis
- verschlüsselt im Dateisystem, Passwort muss übergeben werden
- muss nachinstalliert werden (apt-get -y install encfs)
- kann beliebig ineinander gestapelt werden
- Nutzung z.B. in Cloud ggf. ohne `.encfs6.xml`

Beispiel

- Kunde1 | Kunde2 | Kunde3 | Buchhaltung jeweils mit encfs
- verschlüsseltes /home/stefan mit eCryptFS
- Festplattenverschlüsselung LVM
- hardwareverschlüsselte SSD/SSHD

EXTERNE DATENTRÄGER

- USB-Stick oder SD-Karte verschlüsseln
- Dateisystem mit LUKS
- Verzeichnisse mit encfs
- sensible Daten auslagern
- SD-Karte im Portemonnaie mitführen

Live-Systeme

- starten von CD/DVD oder USB-Stick
- fassen Festplatte nicht an
- können ständig mitgeführt werden
- TAILS: https://tails.boum.org/download/index.de.html
- Porteus / Porteus Kiosk

Dateien verschlüsseln

- mcrypt, GnuPG, OpenSSL
- GnuPG hat standardisiertes Format
- portabel und austauschbar: Linux, *BSD, OS X, Windows
- OpenSSL recht weit verbreitet
- Dateien in tar-Ball packen, verschlüsseln und im Internet ablegen
- Nach der Einreise auf Laptop ziehen
- vor Ausreise wieder löschen

Datensicherung

- Backups! Backups! Backups!
- Offline, Offsite, Archiv!
- Verschlüsseln
- `tar cpf Backup-`date +%y%m%d%H%M`.tar /home/.ecryptfs/stefan/`
- duplicity

Manipulationen erkennen

- Fingerabdruck des Systems erstellen
- AIDE automatisiert dies
- Datenbank von /boot erstellen und vergleichen
- `/etc /bin /sbin /usr/bin /usr/sbin`
- Nach jedem Update aktualisieren
- Prüfung nicht im Live-System sondern via CD/Stick

Manipulationen erkennen

- chkrootkit: Scannt nach Anzeichen von Rootkits
- clamav: freier Virenscanner
- regelmäßige Scans sinnvoll, aber von Live-CD/Stick
- können nicht alle Schadsoftware erkennen

Anwendungen

- so wenig wie möglich installieren
- regelmäßig updates einspielen - sofort
- LibreOffice als Ersatz für MS Office
- nach Möglichkeit vermeiden
- Desktop Environments (KDE, Gnome, LXDE etc.) meiden

FIREJAIL

- SUID-Jail via Kernel Namespaces und seccomp-bpf
- Sandbox bekommt eigene UID, um Zugriffe einzuschränken
- Profile regeln Zugriffe, z.Zt. 630 Stück
- `firejail iridium`
- `firemon --tree`

FIREJAIL

OPTIONEN

- `-bandwidth`
- `-blacklist=dirname-o-filename`
- `-defaultgw=address`
- `-dns=address`
- `-hostname=name`
- `-interface=interface -ip=address`
- `-net=none`
- `-private`
- `-whitelist=dirname-or-filename`

Lynis

- Werkzeug um Betriebssysteme auf Schwachstellen zu überprüfen
- erzeugt Sicherheitsbericht
- stellenweise sehr umfangreich
- Sicherheitsgewinn manchmal marginal oder gar fragwürdig (malware scanner?)

VPN

- Virtual Private Network - verschlüsselt Verbindung zwischen Laptop und Server
- Server zu Hause oder im Unternehmensnetz
- Laptop kann auf Unternehmensserver etc. zugreifen
- Server einfach einrichten z.B. Raspberry PI mit Raspbian, PC mit Ubuntu oder Hardwarelösung (Fritzbox, ASUS)
- Miet-Lösungen
- sichert Verbindungen ins Internet ab
- umgeht Zensurmaßnahmen im Internet
- eventuell verboten und geblockt
- Updates möglichst bei VPN-Verbindung einspielen

Anonymität im Internet

Anonymität

- Internetverbindungen zurückverfolgbar
- TOR anonymisiert diese durch kaskadierende Proxys
- Tor Browser Bundle
- Whonix: Virtuelle Maschine
- TAILS: USB-Stick oder Virtuelle Maschine

Browser

- zentrales Einfallstor für Schadsoftware
- Chromium derzeit am sichersten, AdBlocker installieren (μBlock),
- Midori ist klein und schnell
- auf Flash, Java und Javascript möglichst verzichten (uMatrix, FlashBlock)
- ggf. mehrere Browser einsetzen
- einfaches absichern mit FireJail

NextCloud

- NextCloud: eigenen Cloud-Server aufsetzen
- kann z.B. Google auf Android ersetzen, iOS App verfügbar
- Kalender, Aufgaben, Adressbuch, Dokumentenverwaltung etc.
- Keine Auslieferung der Daten an Google, Apple, Dropbox und Co.
- Betrieb mittels VPN zusätzlich absichern

Virtuelle Maschinen

- VirtualBox `https://www.virtualbox.org/`
- Open Source, Virtuelle Maschine
- Linux, Windows, Android, FreeBSD, NetBSD ...
- virtuelle Maschinen voneinander abgrenzen

AppArmor

- Kernelmodul, steuert Zugriffsrechte der Prozesse
- automatisch installiert
- Profile für bekannte Programme existieren und werden automatisch eingerichtet
- eigene Profile können erstellt werden
- sichert insbesondere komplexe Programme (Thunderbird, Evolution)


yubico
yubico
fido

U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass

U2F Unterstützung

- Google, Dropbox, Github, PAM,
- Wordpress, Django, Ruby on Rails
- OpenSSH, Login, OpenVPN, FreeRADIUS via PAM
- LastPass, Dashlane, Password Safe, Passpack, Password Tote, pwSafe, KeePass

Web.de unterstützt U2F nicht

- OATH-HOTP im Yubikey Personalization Tool einrichten, Secret Key generieren
- KeePass installieren und einrichten, Plugin OtpKeyProv installieren, Secret Key hinterlegen
- sicheres Passwort für Keepass vergeben
- Zufallspasswort (256HEX Bit) generieren und bei Web.de eintragen

  `09137f0ac6627f9e94e2af2342d2610bf20ff0ee929114d27b3629e3823e11ea`
- KeePass mit dem Webbrowser via Plugin verbinden
- KeePass-Datenbank mit Passwort und Token entschlüsseln, Browser holt User/Passwort für Web.de via Plugin aus DB.

- sicherheitsforschung-magdeburg.de
- stefan.schumacher@sicherheitsforschung-magdeburg.de
- sicherheitsforschung-magdeburg.de/publikationen/journal.html

- youtube.de/Sicherheitsforschung
- Twitter: 0xKaishakunin
- Xing: Stefan Schumacher