Chaos Communication Camp 2003

7|8|9|10 August

Mirko Dziadzka

2003-09-17

Inhalt

- Was ist das und warum war ich da?
- Konferenzprogramm
- Fragen

Was ist das und warum war ich da?

- Spiegel: „Cyber-Woodstock auf der Pferdekoppel“
- Official: The Chaos Communication Camp is an international, four-day open-air event for hackers and associated life-forms.

Was ist das und warum war ich da?

- Camp – in der Nähe von Berlin
- in der Tradition von
  - HEU (Hacking at the End of the Universe) 1993 in NL
  - HIP (Hacking in Progress) 1997 in NL
  - CCC (Chaos Communication Camp) 1999 in D
  - HAL (Hacking at Large) 2001 in NL

Was ist das und warum war ich da?

- Zeltplatz auf der grünen Wiese (Pferdekoppel)
- Mit Tagesbesuchern ca. 1800 Leuten

Was ist das und warum war ich da?

- Ein normales Camp?

Was ist das und warum war ich da?

- Ein normales Camp?
- Strom aus Dieselgeneratoren
- Internet über Richtfunk (155Mbit)

Was ist das und warum war ich da?

- DECT Netz
- Eigener Radiosender (UKW + Streaming + DECT)
- Strom und Campnetz über Glasfaser + 100 Mbit in jedes Zelt
- Viel Spass

Konferenz

- 4 Tage
- von 12:00 Uhr bis 0:00 Uhr
- 2 Tracks
- diverse Workshops, etc.
- 50:50 Mix aus technischen und politischen Themen

Andreas Bogk: Why C and UNIX suck for security, and what alternatives we have

- Andreas ist GwydionDylan Entwickler und lästert wie üblich über Unix und C auf dem Niveau des „Unix Hater Handbook“

Andreas Bogk: Why C and UNIX suck for security, and what alternatives we have

- Andreas ist GwydionDylan Entwickler und lästert wie üblich über Unix und C auf dem Niveau des „Unix Hater Handbook“
- Aber: Er hat eine IMHO brauchbare Idee
  - Linux auf L4
  - Dylan soll native Code für x86 unter L4 generieren
  - Dylan um L4 Tasks zu schreiben
  - Nach und nach Ersetzen der Sicherheitskritischen Subsysteme (Filesystem Encryption, SSL Keys, ...) im Linux durch verifizierbare Treiber in Dylan

PNR - The USG/NSA claim for air flight passenger data

- The status quo of the forced delievery of European Passenger name records to the Office of Homeland Security
- Vertrag zwischen USA und Europa
  - einseitige Datenübermittlung
  - widerspricht nationalem Datenschutzrecht (zumindest in D)

John Gilmore: Suing Ashcroft: Anonymity, Right to Travel, Secret Laws

- John Gilmore verklagt die US Regierung, da er als Amerikaner nicht mehr ohne Pass innerhalb der USA vernünftig reisen kann.

- `http://freetotravel.org/`

John Gilmore: Suing Ashcroft: Anonymity, Right to Travel, Secret Laws

- John Gilmore verklagt die US Regierung, da er als Amerikaner nicht mehr ohne Pass innerhalb der USA vernünftig reisen kann.
- `http://freetotravel.org/`
- Durfte auch nicht fliegen, als er einen Button „Suspected Terrorist“ trug.


Suspected
Terrorist

THC tools - amap and hacker tunnel

- Deutsche Hackergruppe „The Hackers Choice“
- `http://www.thc.org`

THC tools - amap and hacker tunnel

- Deutsche Hackergruppe „The Hackers Choice“
- `http://www.thc.org`
- amap: nmap, aber auf Applikationseene

THC tools - amap and hacker tunnel

- Deutsche Hackergruppe „The Hackers Choice“
- `http://www.thc.org`
- amap: nmap, aber auf Applikationseene
- Grenzgaenger: Socks ähnlicher Proxy, der durch so gut wie alles tunneln kann. Auch mit „call home“ Funktionalität.

THC tools - amap and hacker tunnel

- Deutsche Hackergruppe „The Hackers Choice“
- `http://www.thc.org`
- amap: nmap, aber auf Applikationseene
- Grenzgaenger: Socks ähnlicher Proxy, der durch so gut wie alles tunneln kann. Auch mit „call home“ Funktionalität.
- Langsam sollten wir wirklich mal brauchbare IDS in den Proxy Servern aufbauen

Frank Rieger: Navigation Warfare - GPS, Galileo and the limits of trust

- Frank ist der „Information Warfare“ Experte des CCC
- technische Hintergründe
  - Satelitennavigation
  - „Selective Availability“
  - „Differential GPS“
- Wie kann man GPS stören (you really want this if you are on the „receiving end“ of such a GPS guided - aehm - device)
- Wie kann man verhindern, dasss GPS gestört wird?

Frank Rieger: Navigation Warfare - GPS, Galileo and the limits of trust

- Wann kommt Gallileo? Ja, es kommt wirklich!
- Auf welchen Frequenzen?
- Was gibt es in China? Russland?
- `http://www.google.com/search?q=frank+rieger+ccc`

Phenoelit: Cisco Vulnerabilities: Yesterday, Today and Tomorrow - Burning Bridges where we can

- Deutsche Hackergruppe
- Beschäftigen sich seit Jahren mit Cisco Routern (haben leider keine Switches zum Spielen)
- Massenhaft Buffer Overflows und andere Probleme im Cisco IOS
- Mit jedem neuen Feature wiederholt Cisco alle alten Security Probleme

Phenoelit: Cisco Vulnerabilities: Yesterday, Today and Tomorrow - Burning Bridges where we can

- Nette Tools: `http://www.phenoelit.de/`
  - IOS 11.x remote sniffer
  - IOS 11.x remote HTTP exploit

Phenoelit: Hacking Embedded Systems - from Printers to Mobile Phones

- In jedem neuen „OS“ werden die alten Security Probleme wiederholt
- Viele neue Drucker haben heute einen Webserver - mit den üblichen Exploits.
- Auf den Dingern läuft heute JAVA

Phenoelit: Hacking Embedded Systems - from Printers to Mobile Phones

- Ja, die Dinger sind über Web upgradebar.

Phenoelit: Hacking Embedded Systems - from Printers to Mobile Phones

- Ja, die Dinger sind über Web upgradebar.
- Ja, der Loader überprüft die digitale Signatur des neuen Codes beim Upload.

Phenoelit: Hacking Embedded Systems - from Printers to Mobile Phones

- Ja, die Dinger sind über Web upgradebar.
- Ja, der Loader überprüft die digitale Signatur des neuen Codes beim Upload.
- Ja, der Hersteller stellt einen zweiten Classloader (gültig signiert) zur Verfügung, der die Signaturen nicht mehr prüft. *hüstel*

Phenoelit: Hacking Embedded Systems - from Printers to Mobile Phones

- Man kann versuchen einen Drucker zu übernehmen und von dort aus das Netz zu scannen ..

Phenoelit: Hacking Embedded Systems - from Printers to Mobile Phones

- Man kann versuchen einen Drucker zu übernehmen und von dort aus das Netz zu scannen ..
- Merkt das das IDS?

Phenoelit: Hacking Embedded Systems - from Printers to Mobile Phones

- Man kann versuchen einen Drucker zu übernehmen und von dort aus das Netz zu scannen ..
- Merkt das das IDS?
- Oder man verschickt jedes vom Rechner des Chefs gedruckte Dokument an eine externe Adresse ....
- Das nächste sind die Mobile Phones mit Java ...

Fefe: LDAP and OpenLDAP - a second opinion

- Fefes Rant über die Ineffizienz von OpenLDAP
- Details über das LDAP Protokoll
- Details zu tinyldap

Links und Fragen?

- `http://www.ccc.de/camp` (Links auf weitere Doku)
- `ftp://ftp.ccc.de/camp2003/Dokumentation_CamP2003` (ca. 11 GB)
- `http://mirko.dziadzka.net/camp2003` (ein paar schlechte Bilder)

Nächstes Bier & Chips