

Netzwerksniffing mit Wireshark

Ingo Blechschmidt

Augsburger Linux-Infotag

24. März 2012

Zum Mitmachen...

...mit WLAN *WIRESHARK* verbinden!

Mitschneiden von Netzwerkverkehr

Leitfrage:

Wie sehen die Daten aus, die mein Rechner verschickt und empfängt?

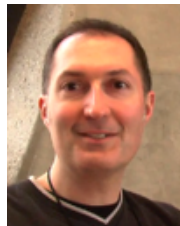


Wozu das?

- Um Netzwerkprotokolle zu verstehen.
- Um Verbindungsprobleme zu diagnostizieren.
- Um das eigene Sicherheitsbewusstsein zu schärfen.
- Um verborgene Hintergrundkommunikation aufzudecken.

Über Wireshark

- Wireshark: freies Werkzeug zum Netzwerksniffing
- erste Veröffentlichung 1998 durch Gerald Combs
- `$ apt-get install wireshark`
- keine Magie – Daten eh im Klartext vorhanden
- Vorsicht: Sicherheitsprobleme in Wireshark selbst
- Alternativen: tcpdump;
begrenzt auch Firefox, Chrome



Gerald Combs

Netzwerkarchitektur

- Versand und Empfang von Netzwerkdaten in einzelnen Paketen
- typische Maximalgröße: 1500 Bytes bei Ethernet
- Adressierungsarten:
 - global: Domainnamen, etwa `luga.de`
 - global: IP-Adressen, etwa `193.99.144.80`
 - lokal: MAC-Adressen, etwa `00:16:76:7d:00:c2`

Live-Vorführung

- 1 Erste Schritte: Ping
Demonstration von ARP, DNS und ICMP
- 2 Start von Google Chrome
DNS-Prefetching, DNS-Tests
- 3 Webseitenaufruf, Pre-Rendering
- 4 unverschlüsselter Login
- 5 ARP-Spoofing (Debian-Paket dsniff)

Bildquellen

- http://smaportal.files.wordpress.com/2009/05/wireshark_icon.png
- <http://www.techiwarehouse.com/userfiles/sniffing2.jpg>
- http://www.soldierx.com/system/files/hdb/gerald_combs.png