FH AACHEN
UNIVERSITY OF APPLIED SCIENCES

Forensische Untersuchung von DSL-Routern

Konrad Albrecht

Lehrgebiet Datennetze, IT-Sicherheit und IT-Forensik

IT Forensik
FH Aachen

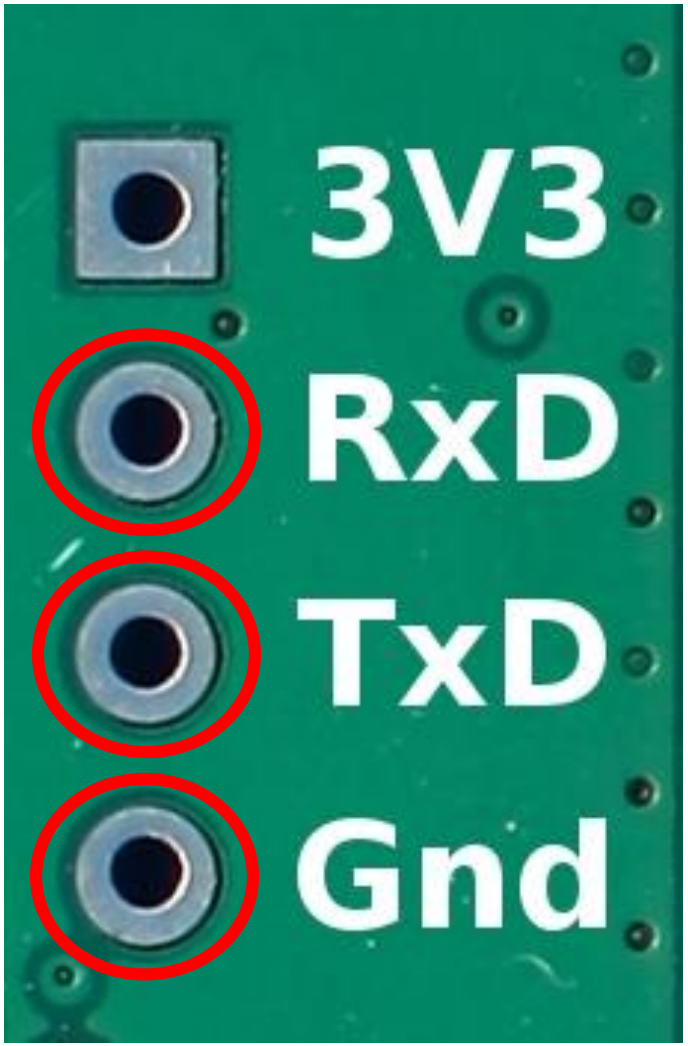
Problemstellung

- Sicherung Kommunikationsdaten
- Passwortschutz
  - Weboberfläche
  - Telnet
- Sicherung erschwert

Vorgehen

- Serielle Schnittstelle
  - Embedded Linux (Busybox)
  - Root-Rechten
  - Alternative zu Chip-Off
- FTDI Chip
- Manuelle Suche
  - Vergleiche ziehen
  - Automatisiertes Tool
- „Zange“ für den Ermittler

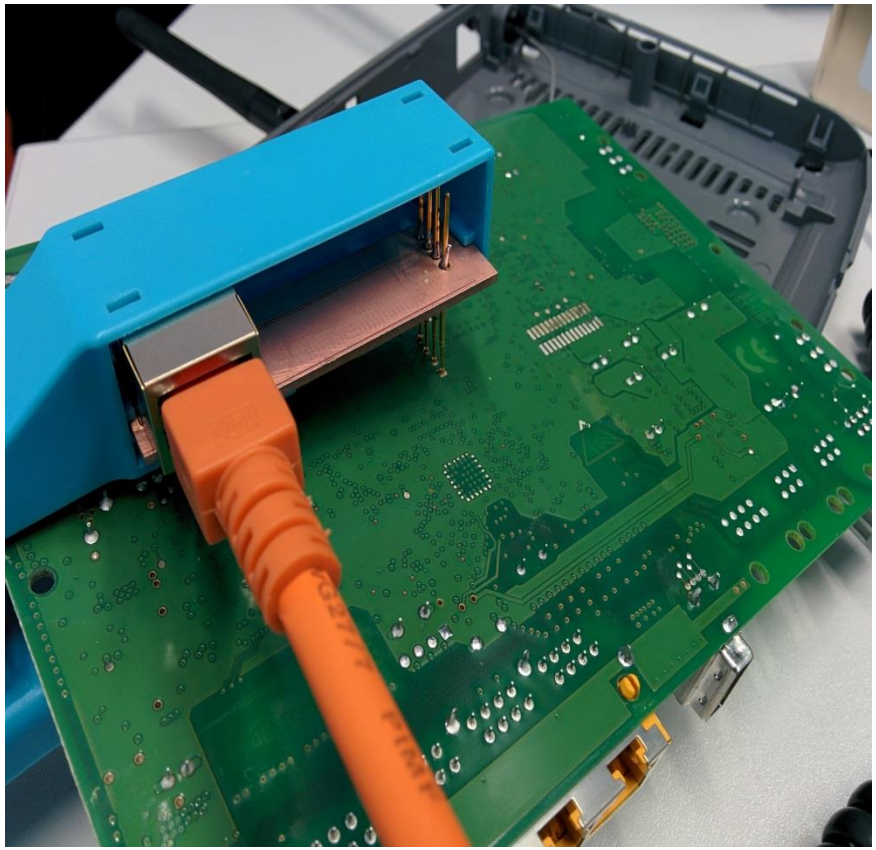
Vorgehen



- RxD Empfang von Daten
- TxD Senden von Daten

Serielle Schnittstelle eines FRITZ!Box DSL-Routers
Quelle: http://www.wehavemorefun.de/fbwiki/images/a/a0/Serielle_Konsole-Bild1.jpg Stand: 27.04.2014

Vorgehen



„Zange“ mit RJ45 Buchse
Quelle: LKA NRW

- 4 Pins zur Vermeidung von Kurzschlüssen
- RJ45 als Signalträger
- FDTI Umwandlung auf USB

Erste Ergebnisse: Ereignisliste

```
21.04.14 17:57:34 Anmeldung an der FRITZ!Box Benutzeroberfläche von IP-Adresse 192.242.242.1.
21.04.14 16:37:05 WLAN-Gerät abgemeldet (2,4 GHz). Name: EpsonStylusSX235W, MAC-Adresse: A4:EE:57:31:B2:BB.
21.04.14 14:51:39 WLAN-Gerät abgemeldet (2,4 GHz). Name: KonradNB-WLAN(2), MAC-Adresse: 00:21:5C:20:13:C7.
21.04.14 14:40:47 WLAN-Gerät angemeldet (2,4 GHz). Name: KonradNB-WLAN(2), IP-Adresse: 192.242.242.3, MAC-Adresse: 00:21
:5C:20:13:C7, Geschwindigkeit 54 MBit/s.
21.04.14 12:06:52 WLAN-Gerät angemeldet (2,4 GHz). Name: EpsonStylusSX235W, IP-Adresse: 192.242.242.8, MAC-Adresse: A4:E
E:57:31:B2:BB, Geschwindigkeit 54 MBit/s.
21.04.14 11:13:48 WLAN-Gerät angemeldet (2,4 GHz). Name: KonradHTCOne, IP-Adresse: 192.242.242.4, MAC-Adresse: 84:7A:88:
56:F2:CE, Geschwindigkeit 54 MBit/s.
21.04.14 11:12:43 WDS-Repeater angemeldet (2,4 GHz). MAC-Adresse: 00:15:0C:E6:6B:41, Geschwindigkeit 54 MBit/s.
21.04.14 11:12:32 WDS-Repeater abgemeldet (2,4 GHz). MAC-Adresse: 00:15:0C:E6:6B:41.
21.04.14 11:12:23 Die Systemzeit wurde erfolgreich aktualisiert von Zeitserver 81.0.124.253.
21.04.14 11:12:18 Internetverbindung wurde erfolgreich hergestellt. IP-Adresse: 80.138.5.14, DNS-Server: 217.0.43.33 und
 217.0.43.17, Gateway: 217.0.116.145, Breitband-PoP: AACX41-erx
21.04.14 11:12:13 WDS-Repeater angemeldet (2,4 GHz). MAC-Adresse: 00:15:0C:E6:6B:41, Geschwindigkeit 54 MBit/s.
21.04.14 11:12:06 DSL ist verfügbar (DSL-Synchronisierung besteht mit 3456/448 kbit/s).
```

- Ereignisliste ist nach Neustart nicht mehr vorhanden!

Erste Ergebnisse: Telefonbuch

```
# cat /var/flash/phonebook
<?xml
version="1.0" encoding="utf-8"><phonebook><contact><category /><person><realName
>AVM Ansage (HD)</realName></person><telephony
nid="1"><number prio="1" type="work" quickdial="99" id="0">500@hd-telefonie.avm.
de</number></telephony><services /><setup /><uniqueid>0</uniqueid></contact><con
tact><category /><person><realName>HD-Musik</realName></person><telephony
tact><category>0</category><person><realName>Konrad</realName></person><telephon
y
nid="2"><number type="home" prio="1" id="0" quickdial="66">123456</number><numbe
r
type="mobile" prio="0" id="1">7890</number></telephony><services /><setup /><mod
_time>1543</mod_time><uniqueid>10</uniqueid></contact></phonebook><uniqueid>13</
nid="2"><number type="home" prio="1" id="0" quickdial="66">123456</number><numbe
r
type="mobile" prio="0" id="1">7890</number></telephony><services /><setup /><mod
_time>1543</mod_time><uniqueid>10</uniqueid></contact></phonebook><uniqueid>13</
uniqueid><featureflags>8</featureflags><phonebook
owner="255"><contact><category /><person><realName>Alle (Rundruf)</realName></pe
rson><telephony
nid="1"><number type="intern" prio="1" id="0">9</number></telephony><services />
```

Erste Ergebnisse: DNS Einträge

```
# cat /var/tmp/dnsddebug.txt
servers:
 + 192.168.180.1:53
 + 192.168.180.2:53
allowedv4:
 192.242.242.0 255.255.255.224 (0.242.242.192.in-addr.arpa)
 169.254.0.0 255.255.0.0 (254.169.in-addr.arpa)
allowedv6:
localinfo:
```

```
KonradHTCOne.fritz.box (none):
    192.242.242.4
        NB-WLAN.fritz.box (none):
    192.242.242.6
KonradPC-LAN.fritz.box (none):
    192.242.242.1
WIN-4TQ9RSBUJEK.fritz.box (none):
    192.242.242.14 (dynamic)
```

```
        -PC.fritz.box (none):
    192.242.242.13 (dynamic)
        PC-LAN.fritz.box (none):
    192.242.242.5
KonradHTCOne.fritz.box (none):
    192.242.242.4
        NB-WLAN.fritz.box (none):
    192.242.242.6
KonradPC-LAN.fritz.box (none):
    192.242.242.1
WIN-4TQ9RSBUJEK.fritz.box (none):
    192.242.242.14 (dynamic)
```

Erste Ergebnisse: Sicherung

- USB Stick
  - Automatisch eingebunden
- Webserver
  - Umleitung der Startseite

Vielen Dank

Vielen Dank für Ihre Aufmerksamkeit!

Konrad Albrecht

Lehrgebiet Datennetze, IT-Sicherheit
und IT-Forensik