

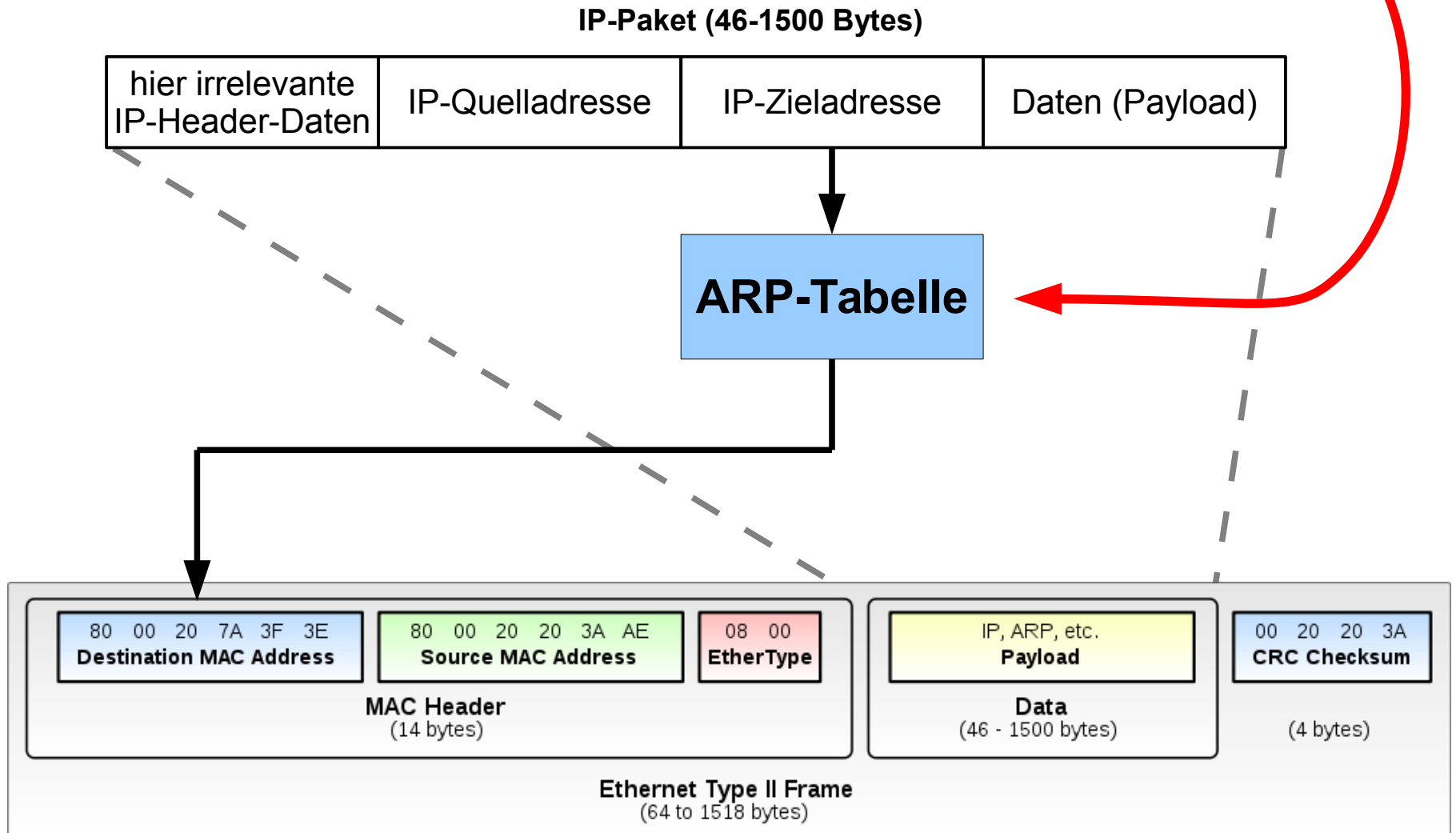
ARP-Spoofing & Co.

- ▣ Frame 9 (60 bytes on wire, 60 bytes captured)
 - Arrival Time: May 9, 2007 17:11:03.225513000
 - [Time delta from previous packet: 0.000393000 seconds]
 - [Time since reference or first frame: 9.655979000 seconds]
 - Frame Number: 9
 - Packet Length: 60 bytes
 - Capture Length: 60 bytes
 - [Frame is marked: False]
 - [Protocols in frame: eth:arp]
 - [Coloring Rule Name: ARP]
 - [Coloring Rule String: arp]
- ▣ Ethernet II, Src: r-irene.grupp.private (00:0e:a6:73:5e:55), Dst: r-andreas.grupp.private (00:30:05:42:33:eb)
 - ▣ Destination: r-andreas.grupp.private (00:30:05:42:33:eb)
 - ▣ Source: r-irene.grupp.private (00:0e:a6:73:5e:55)
 - Type: ARP (0x0806)
 - Trailer: 00000000000000000000000000000000
- ▣ Address Resolution Protocol (reply)
 - Hardware type: Ethernet (0x0001)
 - Protocol type: IP (0x0800)
 - Hardware size: 6
 - Protocol size: 4
 - Opcode: reply (0x0002)
 - Sender MAC address: r-irene.grupp.private (00:0e:a6:73:5e:55)
 - Sender IP address: r-irene.grupp.private (172.16.0.130)
 - Target MAC address: r-andreas.grupp.private (00:30:05:42:33:eb)
 - Target IP address: r-andreas.grupp.private (172.16.0.131)

Die Hintergründe & ...

```
0000  00 30 05 42 33 eb 00 0e a6 73 5e 55 08 06 00 01  .0.B3... .sAU...
0010  08 00 06 04 00 02 00 0e a6 73 5e 55 ac 10 00 82  .....sAU...
0020  00 30 05 42 33 eb ac 10 00 83 00 00 00 00 00 00  .0.B3... .....
0030  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```

Address Resolution Protokoll

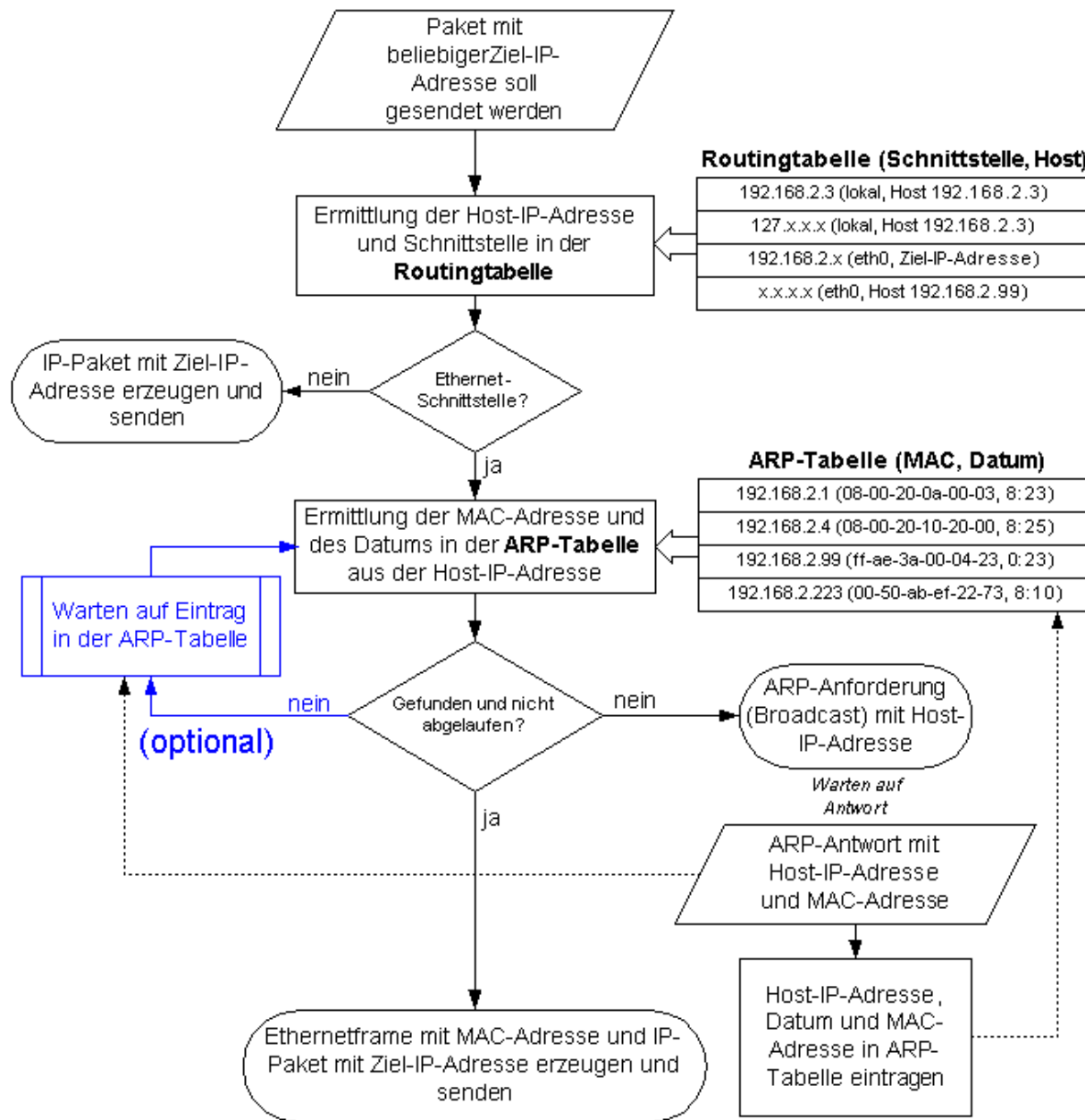


| No. ↓ | Time | Source | Destination | Protocol | Info |
|---|----------|----------------|-------------------|----------|---------------------------------------|
| 1 | 0.000000 | 00:30:05:40:51 | ff:ff:ff:ff:ff:ff | ARP | Who has 172.16.0.3? Tell 172.16.0.131 |
| 2 | 0.000838 | 00:09:52:01:21 | 00:30:05:40:51 | ARP | 172.16.0.3 is at 00:09:52:01:21:3a |
| > Frame 1 (42 bytes on wire, 42 bytes captured) > Ethernet II, Src: 00:30:05:40:51:33 (00:30:05:40:51:33), Dst: ff:ff:ff:ff:ff:ff (ff:ff:ff:ff:ff:ff) > Address Resolution Protocol (request) Hardware type: Ethernet (0x0001) Protocol type: IP (0x0800) Hardware size: 6 Protocol size: 4 Opcode: request (0x0001) [Is gratuitous: False] Sender MAC address: 00:30:05:40:51:33 (00:30:05:40:51:33) Sender IP address: 172.16.0.131 (172.16.0.131) Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00) Target IP address: 172.16.0.3 (172.16.0.3) | | | | | |

ARP-Request

| No. ↓ | Time | Source | Destination | Protocol | Info |
|---|----------|----------------|-------------------|----------|---------------------------------------|
| 1 | 0.000000 | 00:30:05:40:51 | ff:ff:ff:ff:ff:ff | ARP | Who has 172.16.0.3? Tell 172.16.0.131 |
| 2 | 0.000838 | 00:09:52:01:21 | 00:30:05:40:51 | ARP | 172.16.0.3 is at 00:09:52:01:21:3a |
| > Frame 2 (60 bytes on wire, 60 bytes captured) > Ethernet II, Src: 00:09:52:01:21:3a (00:09:52:01:21:3a), Dst: 00:30:05:40:51:33 (00:30:05:40:51:33) > Address Resolution Protocol (reply) Hardware type: Ethernet (0x0001) Protocol type: IP (0x0800) Hardware size: 6 Protocol size: 4 Opcode: reply (0x0002) [Is gratuitous: False] Sender MAC address: 00:09:52:01:21:3a (00:09:52:01:21:3a) Sender IP address: 172.16.0.3 (172.16.0.3) Target MAC address: 00:30:05:40:51:33 (00:30:05:40:51:33) Target IP address: 172.16.0.131 (172.16.0.131) | | | | | |

ARP-Reply



Windows:
`route PRINT`
Linux:
`route -n`
`ip route show`

Windows:
`arp -a`
Linux:
`arp -n`
`ip neigh show`

Beispiel unter Windows (cmd.exe)

```
C:\Dokumente und Einstellungen\Administrator>arp -a
```

```
Schnittstelle: 172.16.0.201 --- 0x2
Internetadresse      Physikal. Adresse      Typ
172.16.0.1           00-0d-88-fc-c0-5f      dynamisch
```

```
C:\Dokumente und Einstellungen\Administrator>ping tk
```

```
Ping tk.grupp.private [172.16.0.3] mit 32 Bytes Daten:
```

```
Antwort von 172.16.0.3: Bytes=32 Zeit=8ms TTL=64
Antwort von 172.16.0.3: Bytes=32 Zeit=1ms TTL=64
Antwort von 172.16.0.3: Bytes=32 Zeit=1ms TTL=64
Antwort von 172.16.0.3: Bytes=32 Zeit=1ms TTL=64
```

```
Ping-Statistik für 172.16.0.3:
```

```
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 1ms, Maximum = 8ms, Mittelwert = 2ms
```

```
C:\Dokumente und Einstellungen\Administrator>arp -a
```

```
Schnittstelle: 172.16.0.201 --- 0x2
Internetadresse      Physikal. Adresse      Typ
172.16.0.1           00-0d-88-fc-c0-5f      dynamisch
172.16.0.3           00-09-52-01-21-3a      dynamisch
```

Löst im Hintergrund zuerst einen DNS- und anschließend einen ARP-Request aus. Erst anschließend ICMP!

Eigene MAC-Adresse:

00:04:c1:c4:67:80

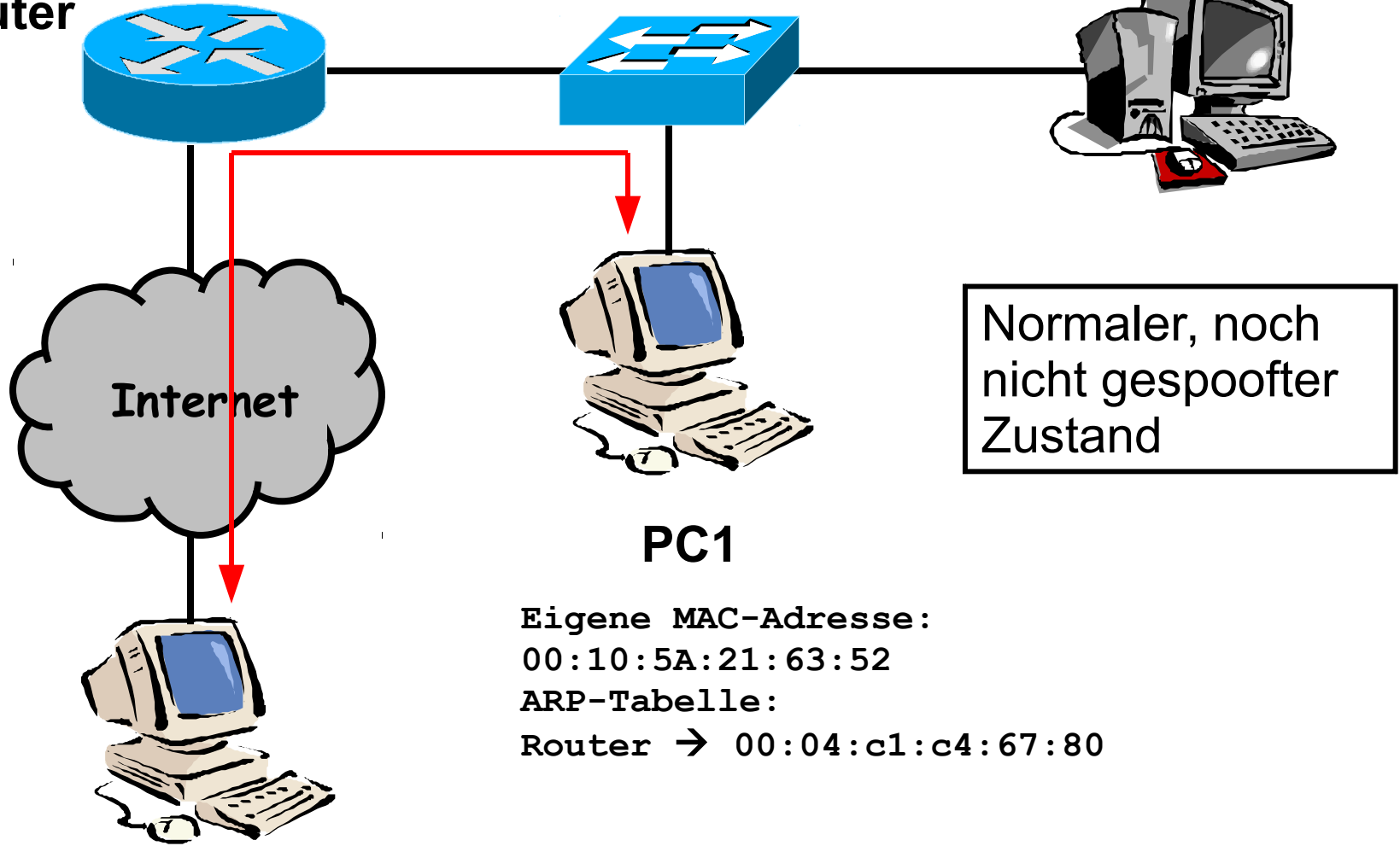
ARP-Tabelle:

PC1 → 00:10:5A:21:63:52

PC2 - Angreifer

08:00:09:C2:E3:CA

Router



Normaler, noch
nicht gespoofter
Zustand

PC1

Eigene MAC-Adresse:

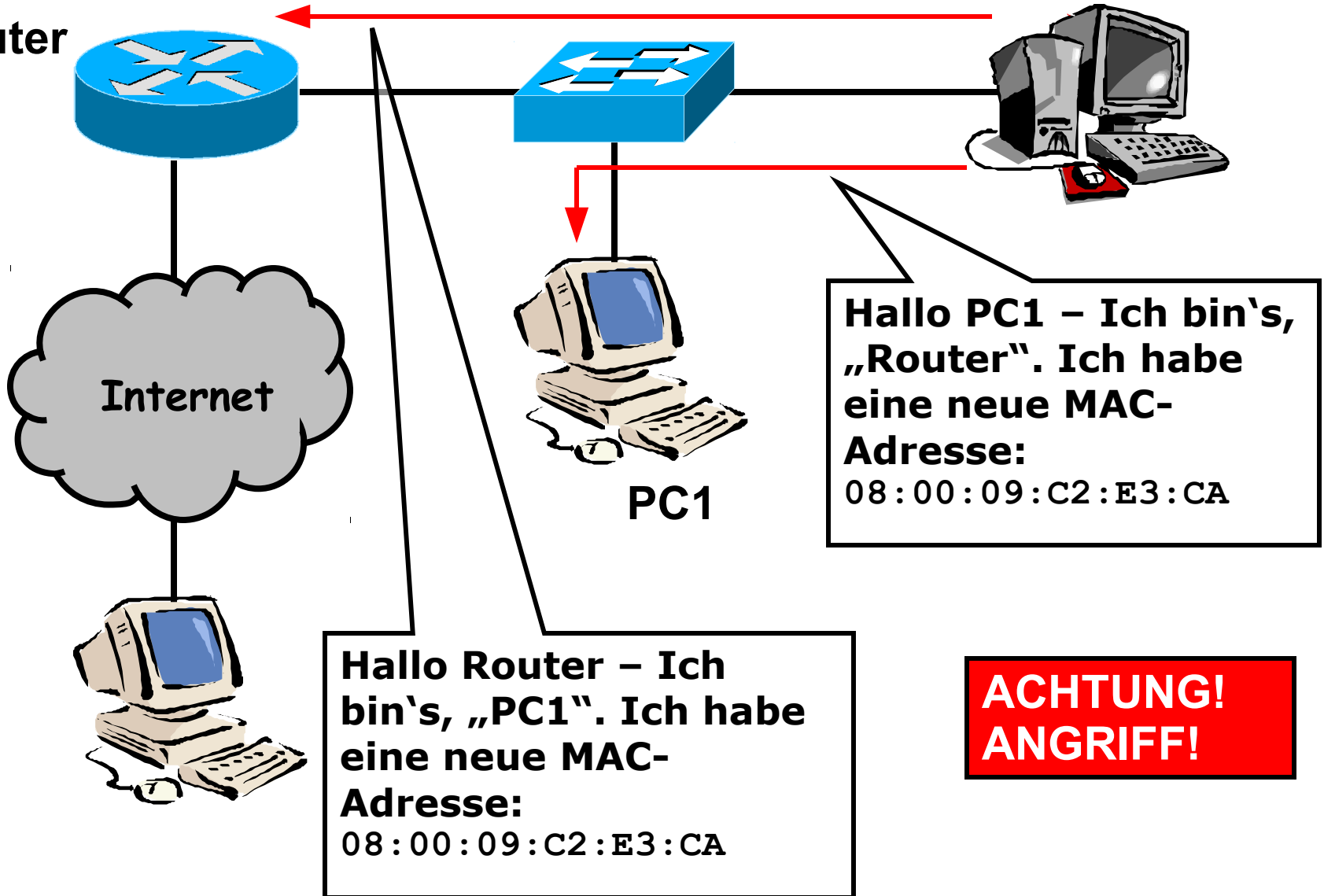
00:10:5A:21:63:52

ARP-Tabelle:

Router → 00:04:c1:c4:67:80

PC2 - Angreifer

Router



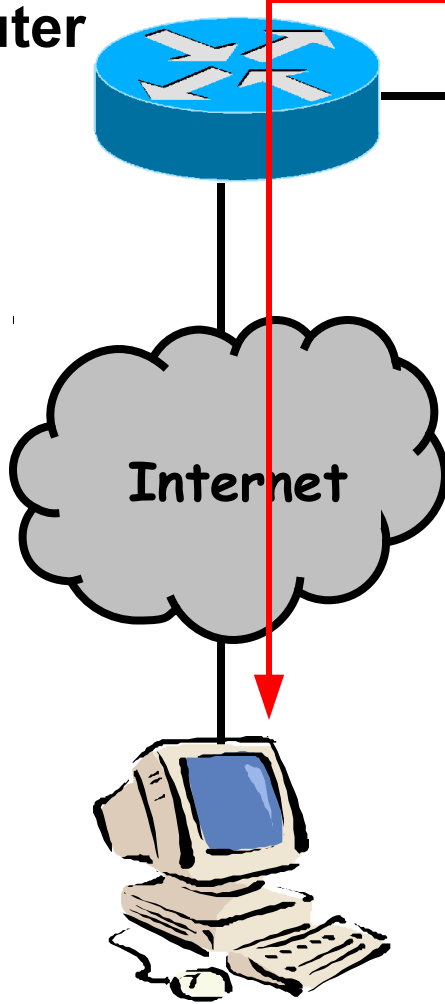
Eigene MAC-Adresse:

00:04:c1:c4:67:80

ARP-Tabelle:

PC1 → 08:00:09:C2:E3:CA

Router



PC1

Eigene MAC-Adresse:

00:10:5A:21:63:52

ARP-Tabelle:

Router → 08:00:09:C2:E3:CA

PC2 - Angreifer

08:00:09:C2:E3:CA



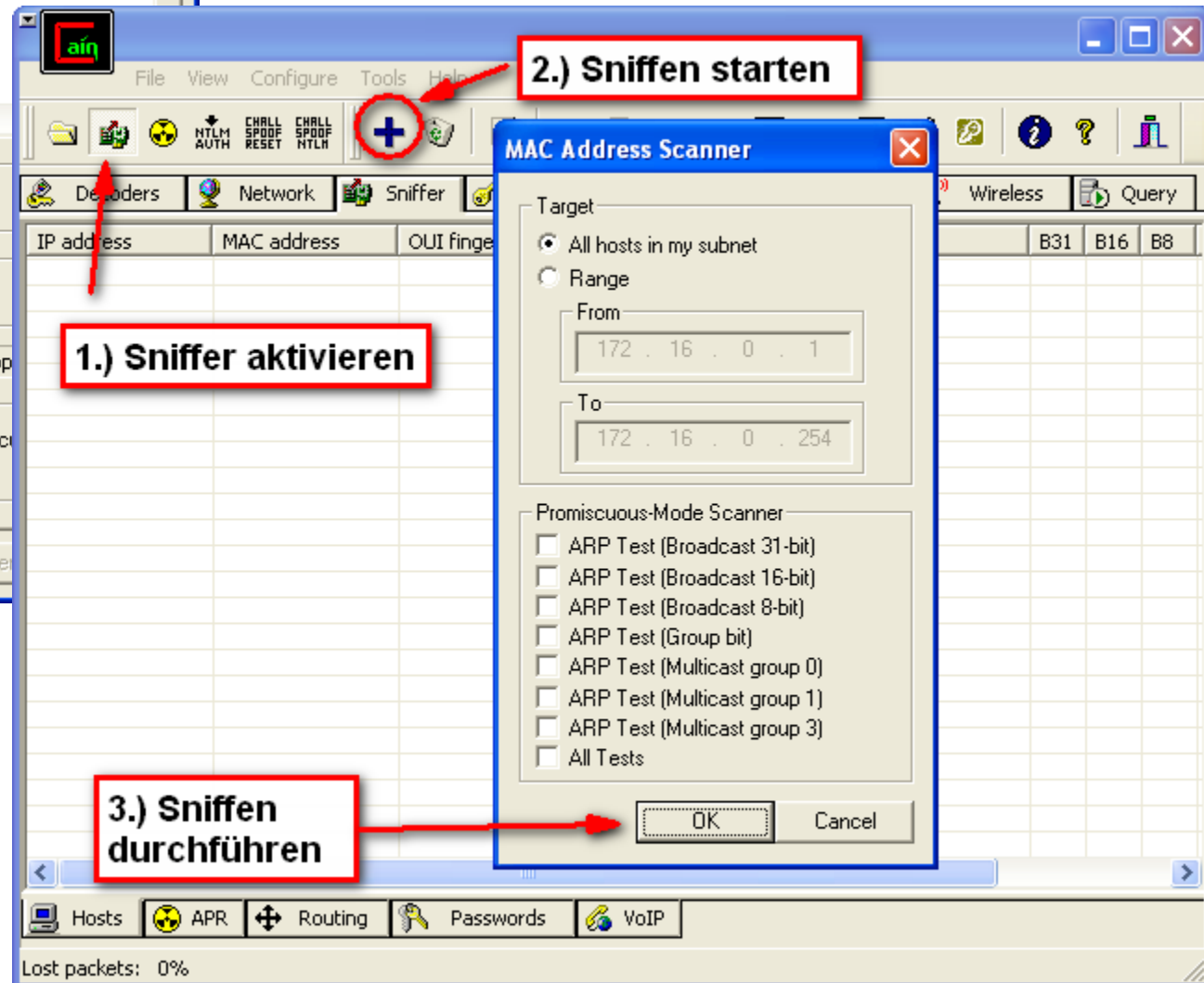
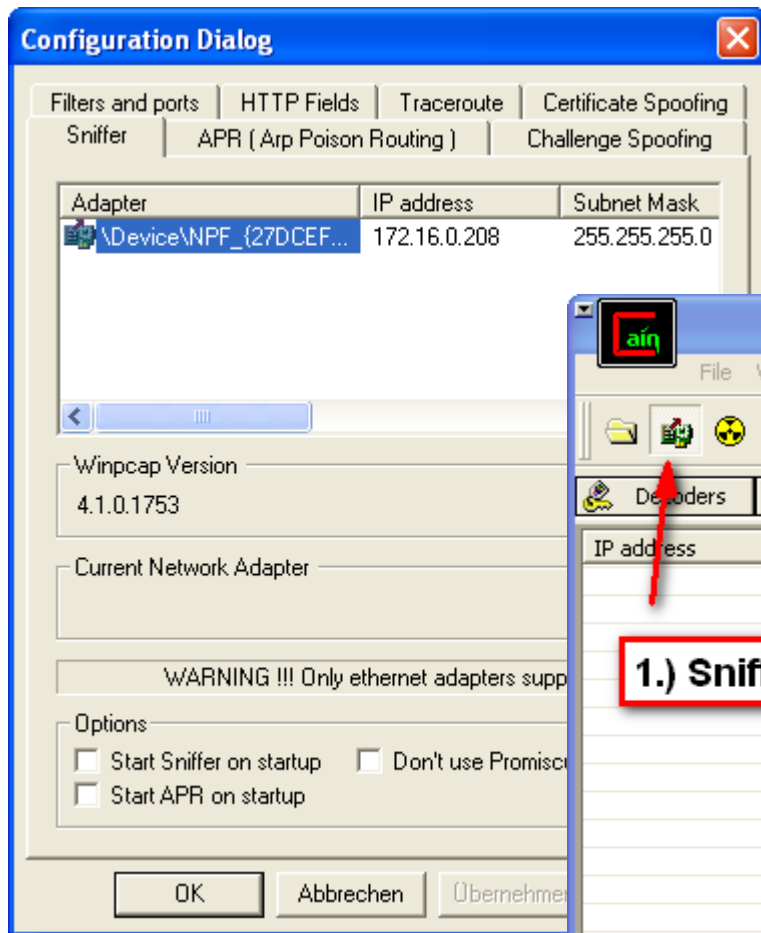
Reingefallen!!
Angegriffener
Zustand

Merke: Der Switch wurde nicht angegriffen – der arbeitet wie er soll!

Tools für ARP-Spoofing

- Cain & Abel – Windows only
 - basiert auf WinPcap-Library (enthalten)
 - relativ einfach zu bedienen
 - einige andere "Features" um das Fürchten zu Lernen
- Ettercap – für mehrere Plattformen
 - basiert auch auf Pcap-Library (muss unter Windows gesondert installiert werden)
 - ebenfalls viele weitere "Features"
 - Tutorial z.B. unter <http://openmaniak.com/ettercap.php>
- Interceptor NG – <http://interceptor.nerf.ru/>

Cain & Abel



Cain & Abel

The screenshot shows the main window of Cain & Abel with the 'Sniffer' tab selected. A red box highlights the '+' icon in the toolbar, labeled '3.) "Opfer"-Bestimmung'. Another red box highlights the 'APR' icon in the bottom toolbar, labeled '2.) In oberen Bereich klicken'. A third red box highlights the 'APR' icon in the bottom toolbar, labeled '1.) Auf ARP-Poisoning Reiter umschalten'. A fourth red box highlights the 'OK' button in the 'New ARP Poison Routing' dialog, labeled '5.) Auswahl beenden'. The dialog also contains a warning message and two tables of IP addresses and MAC addresses.

3.) "Opfer"-Bestimmung

2.) In oberen Bereich klicken

1.) Auf ARP-Poisoning Reiter umschalten

4.) Einen Host links, ein od. mehrere Hosts rechts auswählen

5.) Auswahl beenden

New ARP Poison Routing

WARNING !!!

APR enables you to hijack IP traffic between the selected host on the left list and all selected hosts on the right list in both directions. If a selected host has routing capabilities WAN traffic will be intercepted as well. Please note that since your machine has not the same performance of a router you could cause DoS if you set APR between your Default Gateway and all other hosts on your LAN.

| IP address | MAC | Hostname |
|--------------|--------------|----------|
| 172.16.0.1 | 000D88FCC05F | |
| 172.16.0.2 | 000D88C9B297 | |
| 172.16.0.3 | 00095201213A | |
| 172.16.0.130 | 0030054233EB | |
| 172.16.0.131 | 003005405133 | |
| 172.16.0.132 | 000F1FCA76DC | |
| 172.16.0.140 | 0021708866A7 | |
| 172.16.0.145 | 000E35861188 | |

| IP address | MAC | Hostname |
|--------------|--------------|----------|
| 172.16.0.145 | 000E35861188 | |
| 172.16.0.140 | 0021708866A7 | |
| 172.16.0.132 | 000F1FCA76DC | |
| 172.16.0.131 | 003005405133 | |
| 172.16.0.130 | 0030054233EB | |
| 172.16.0.3 | 00095201213A | |
| 172.16.0.2 | 000D88C9B297 | |

Cain & Abel

1.) ARP-Poisoning aktivieren

2.) Liste der abgehörten Verbindungen füllt sich

| Status | IP address | MAC address | Packets -> | <- Packets | MAC address | IP address |
|-----------|------------|--------------|------------|------------|--------------|--------------|
| Poisoning | 172.16.0.1 | 000D88FCC05F | 240 | 271 | 003005405133 | 172.16.0.131 |

| Status | IP address | MAC address | Packets -> | <- Packets | MAC address | IP address |
|--------------|--------------|--------------|------------|------------|--------------|----------------|
| Full-routing | 95.129.58.33 | 000D88FCC05F | 18 | 20 | 003005405133 | 172.16.0.131 |
| Full-routing | 172.16.0.131 | 003005405133 | 8 | 8 | 000D88FCC05F | 208.68.163.220 |
| Full-routing | 172.16.0.131 | 003005405133 | 1 | 1 | 000D88FCC05F | 99.244.31.199 |
| Full-routing | 172.16.0.131 | 003005405133 | 1 | 1 | 000D88FCC05F | 114.37.193.39 |
| Full-routing | 172.16.0.131 | 003005405133 | 1 | 1 | 000D88FCC05F | 134.208.2.165 |
| Full-routing | 172.16.0.131 | 003005405133 | 1 | 1 | 000D88FCC05F | 87.5.49.8 |
| Full-routing | 172.16.0.131 | 003005405133 | 1 | 1 | 000D88FCC05F | 71.76.63.89 |
| Full-routing | 172.16.0.131 | 003005405133 | 1 | 1 | 000D88FCC05F | 195.19.148.195 |
| Half-routing | 172.16.0.131 | 003005405133 | 4 | 0 | 000D88FCC05F | 188.18.216.95 |

Configuration / Routed Packets

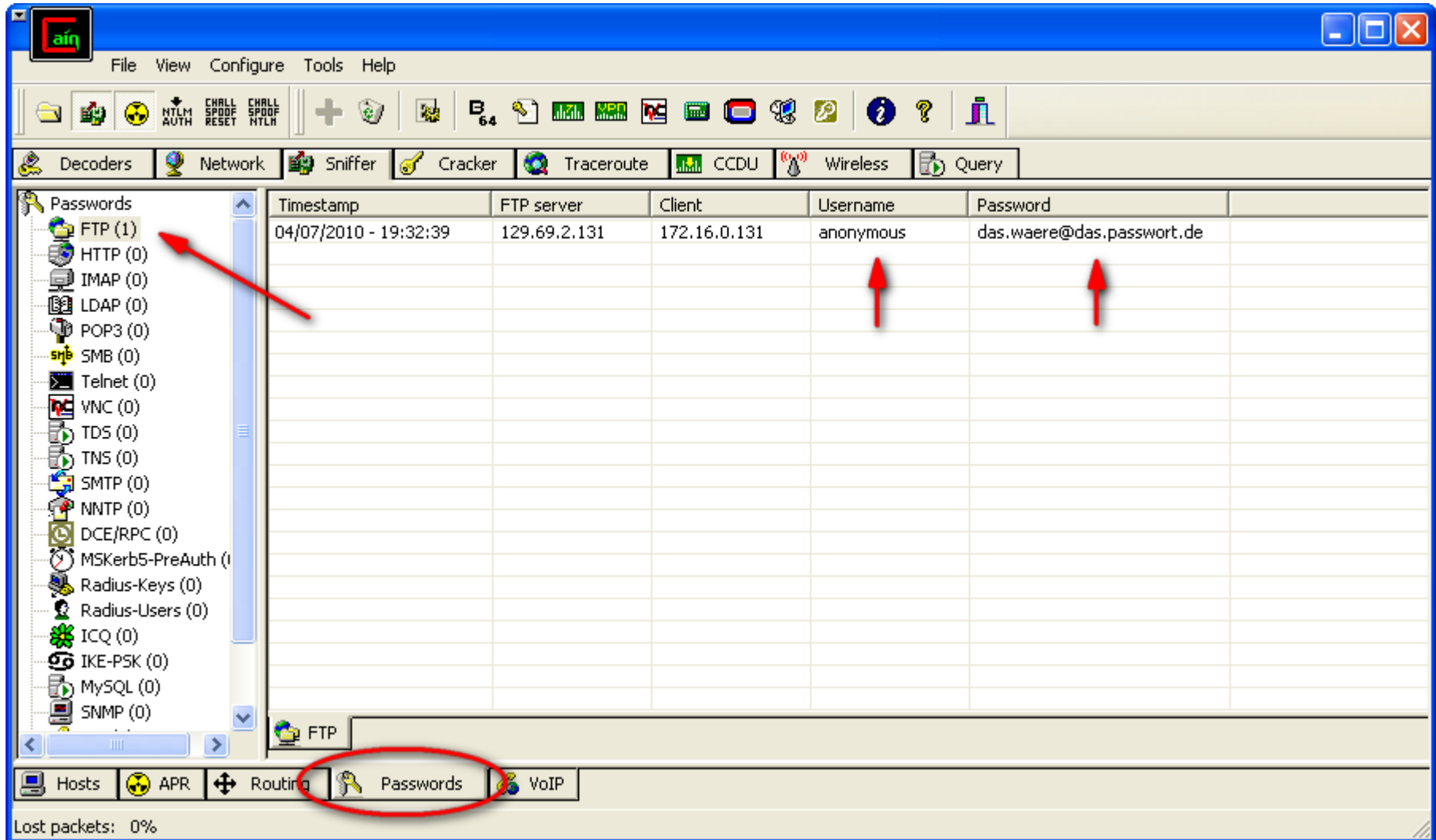
Hosts | ARP | Routing | Passwords | VoIP

Lost packets: 0%

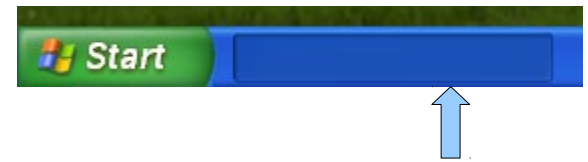
Cain & Abel

```
andreas@r-andreas:~> ip neigh show
172.16.0.1 dev eth0 lladdr 00:0d:88:fc:c0:5f REACHABLE
andreas@r-andreas:~> ip neigh show
172.16.0.1 dev eth0 lladdr 00:0c:29:c0:85:f6 REACHABLE
andreas@r-andreas:~> ftp anonymous@ftp.uni-stuttgart.de
Connected to ftp.uni-stuttgart.de.
220 ProFTPD 1.2.9 Server (Debian) [infolms]
331 Anonymous login ok, send your complete email address as your password.
Password:
230-
230-           We have focussed our ftp-offer on a small set of data.
230-           If you miss a directory or encounter any problems
230-           please feel free to contact us at ftp@ftp.uni-stuttgart.de
230-
230-           Welcome to ftp.uni-stuttgart.de, the
230-           ***** I N F O and S O F T Server *****
230-           Rechenzentrum Universitaet Stuttgart
230 Anonymous access granted, restrictions apply.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Cain & Abel



Cain & Abel



Grundtarnung
in Taskleiste

- Ggf. über die Ignore-List des Virens scanners "verbergen"
- Hotkeys:
 - Alt + Del → Cain-Fenster verstecken
 - Alt + PgDown → In System-Tray minimieren
 - Alt + PgUp → Cain-Fenster restaurieren
- Abel kann als Remote-Service für "diverse Dinge" (auch in anderem Subnetz) installiert werden.



Ettercap mit Kali-Linux

- Um später auch SSL-Hijacking durchführen zu können ist Anpassung der Konfiguration `/etc/etter.conf` an zwei Stellen notwendig!

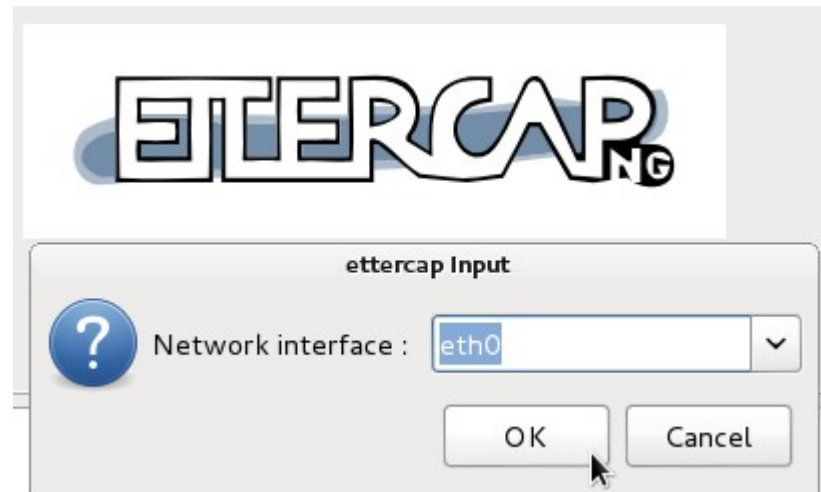
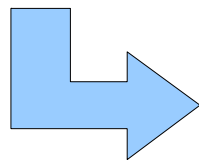
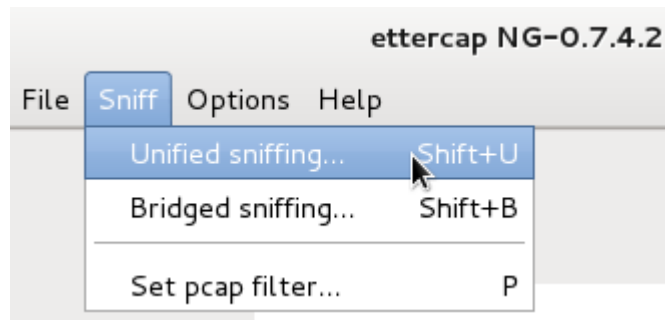
```
[privs]
ec_uid = 0      # nobody is the default
ec_gid = 0      # nobody is the default
```

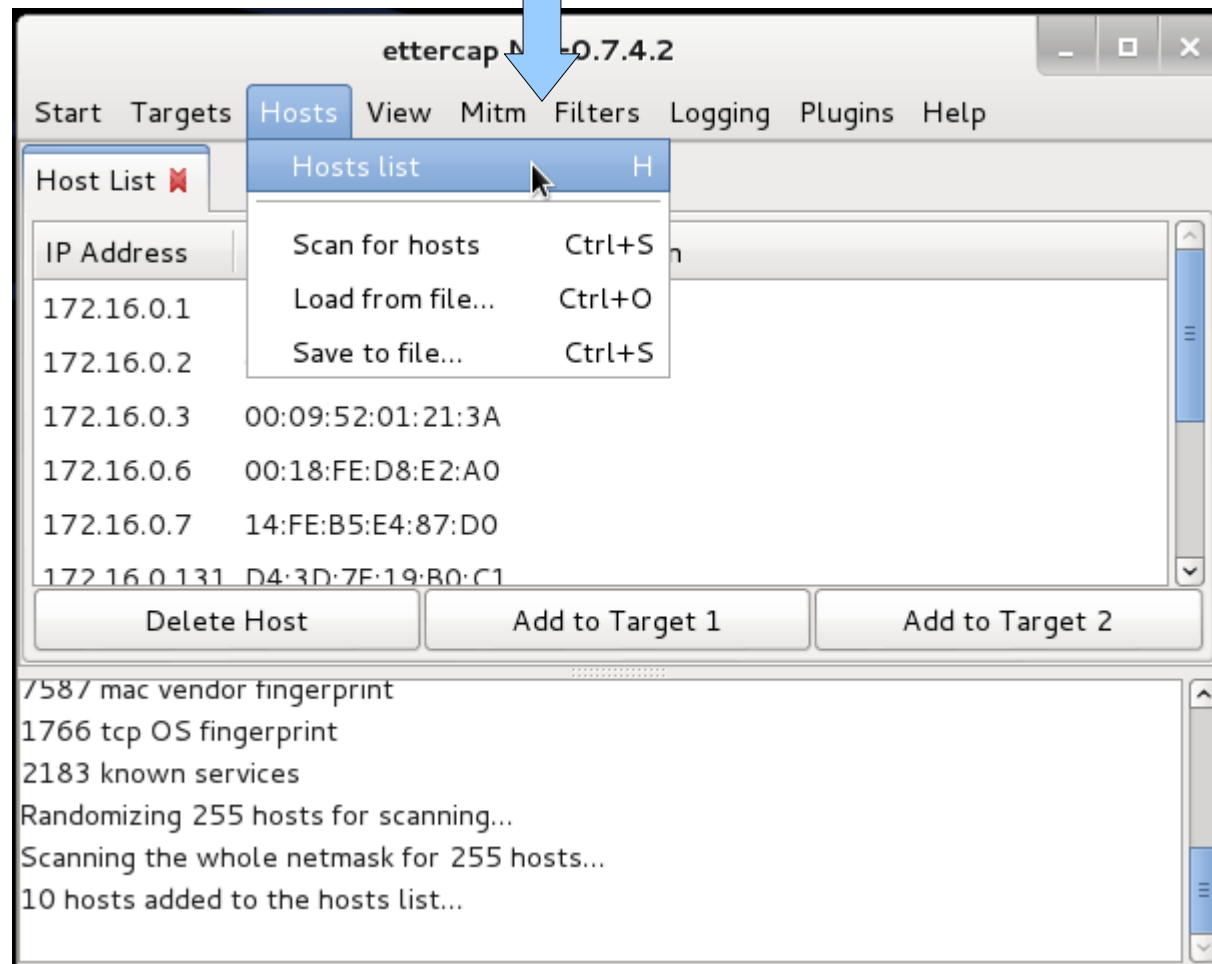
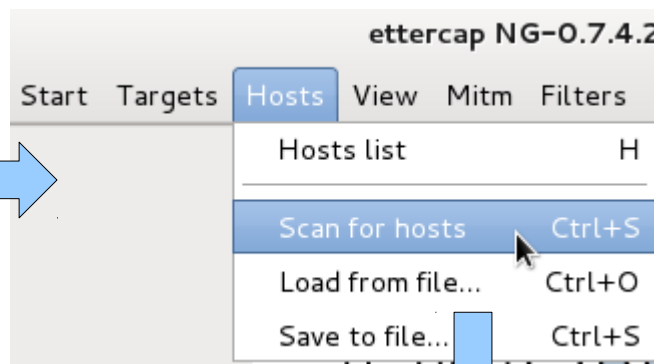
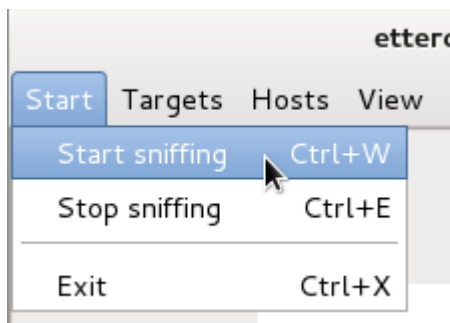
```
# if you use iptables:
redir_command_on = "ip...
redir_command_off = "ip...
```

- `echo 1 > /proc/sys/net/ipv4/ip_forward`

Ettercap mit Kali-Linux

- Ober Menüleiste ganz links ...
- Applications → Kali-Linux → Sniffing/Spoofing → Network Sniffers → ettercap-graphical





ettercap NG-0.7.4.2

Start Targets Hosts View Mitm Filters Logging Plugins Help

Host List

| IP Address | MAC Address | Description |
|--------------|-------------------|-------------|
| 172.16.0.7 | 14:FE:B5:E4:87:D0 | |
| 172.16.0.131 | D4:3D:7E:19:B0:C1 | |
| 172.16.0.149 | 5C:26:0A:77:4D:67 | |
| 172.16.0.200 | 00:0C:29:B6:B7:E1 | |
| 172.16.0.204 | D0:DF:9A:CF:ED:9D | |
| 172.16.0.254 | 52:54:00:21:FE:B3 | |

Delete Host Add to Target 1 Add to Target 2

2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
10 hosts added to the hosts list...
Host 172.16.0.200 added to TARGET1
Host 172.16.0.254 added to TARGET2

ettercap NG-0.7.4.2

View Mitm Filters Logging PL

- Arp poisoning...
- Icmp redirect...
- Port stealing...
- Dhcp spoofing...
- Stop mitm attack(s)

MITM Attack: ARP Poisoning (as nobody)

Optional parameters

- ☒ Sniff remote connections.
- ☐ Only poison one-way.

OK Cancel



Dieser Verbindung wird nicht vertraut

Sie haben Firefox angewiesen, eine gesicherte Verbindung zu **lehrerfortbildung-bw.de** aufzubauen, es kann aber nicht überprüft werden, ob die Verbindung sicher ist.

Wenn Sie normalerweise eine gesicherte Verbindung aufbauen, weist sich die Website mit einer vertrauenswürdigen Identifikation aus, um zu garantieren, dass Sie die richtige Website besuchen. Die Identifikation dieser Website dagegen kann nicht bestätigt werden.

Was sollte ich tun?

Falls Sie für gewöhnlich keine Probleme mit dieser Website haben, könnte dieser Fehler bedeuten, dass jemand die Website fälscht. Sie sollten in dem Fall nicht fortfahren.

Diese Seite verlassen

- Technische Details
- ▼ Ich kenne das Risiko

Wenn Sie wissen, warum dieses Problem auftritt, können Sie Firefox anweisen, der Identifikation dieser Website zu vertrauen. **Selbst wenn Sie der Website vertrauen, kann dieser Fehler bedeuten, dass jemand ihre Verbindung manipuliert.**

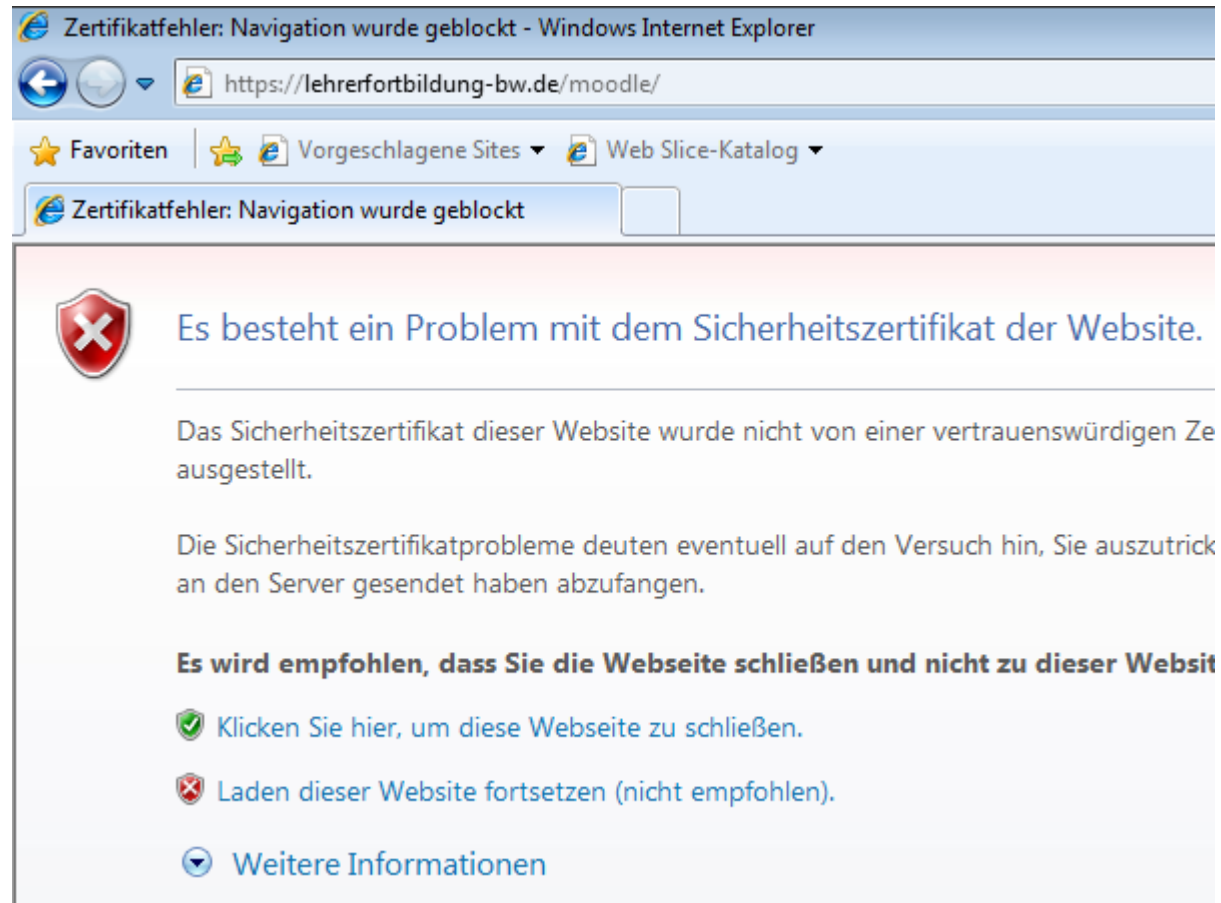
Fügen Sie keine Ausnahme hinzu, außer Sie wissen, dass es einen guten Grund dafür gibt, warum diese Website keine vertrauenswürdige Identifikation verwendet.

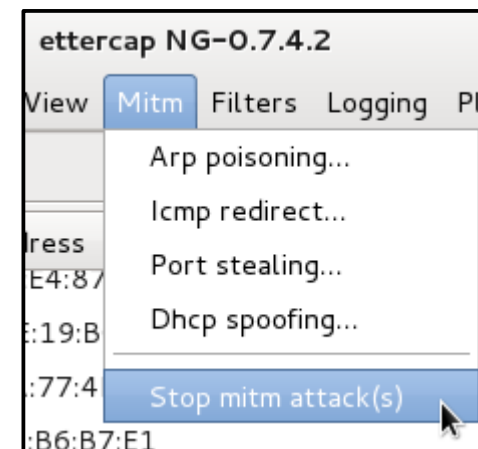
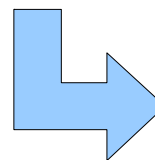
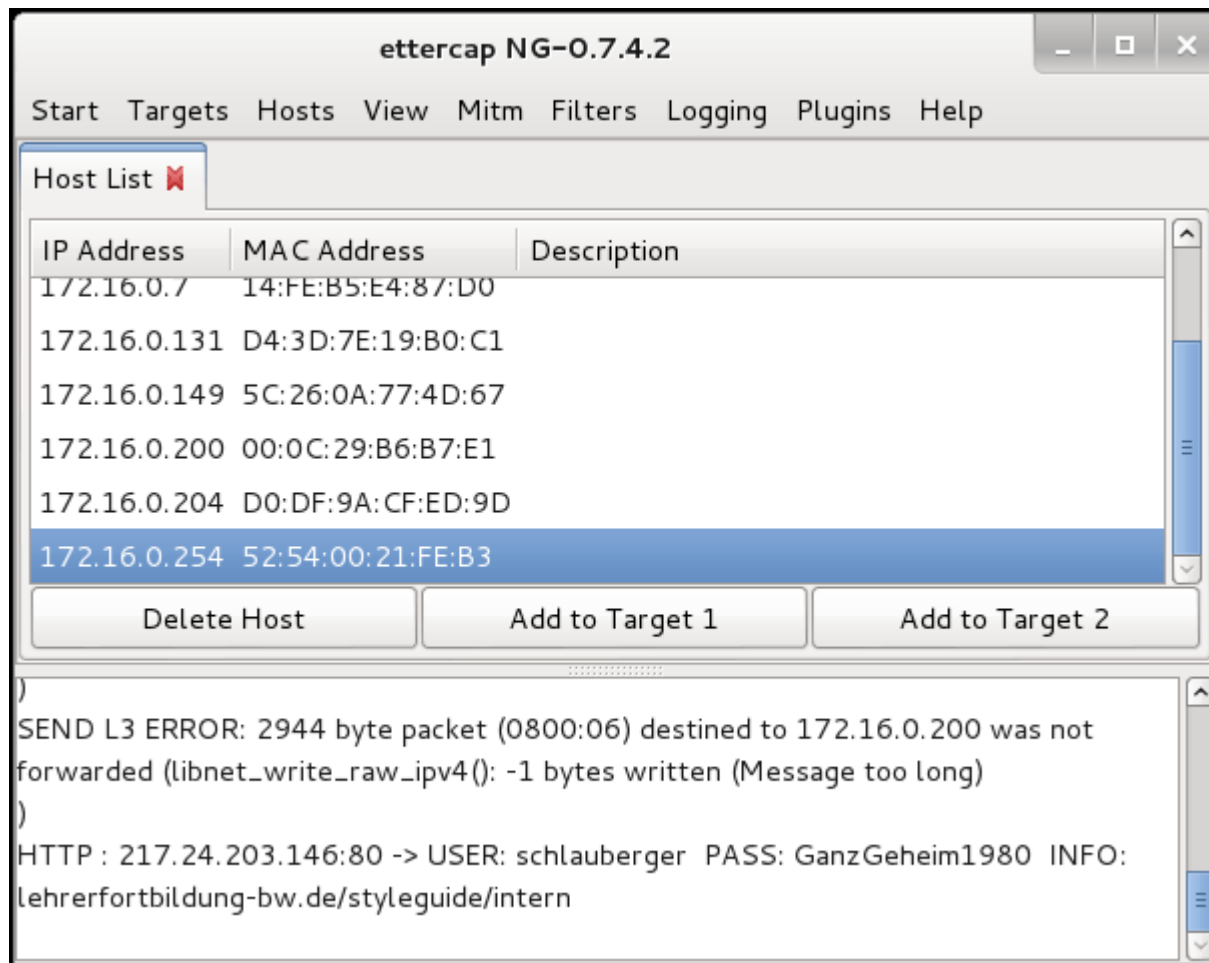
Ausnahmen hinzufügen...

**Hmmm ... das ist
zwar komisch ...**

... aber mal Hand auf's Herz ...

... wie oft haben Sie so was schon „weggeklickt“?





Zusätzliche Formularfelder

- Im HTML-Quellcode den Namen des jeweiligen Input-Elements nachschauen

Hie das
Beispiel von
GMX ... wobei
dort leider auch
wegen https
das Sniffen
durch den
Zertifikats-
fehlers auffällt.

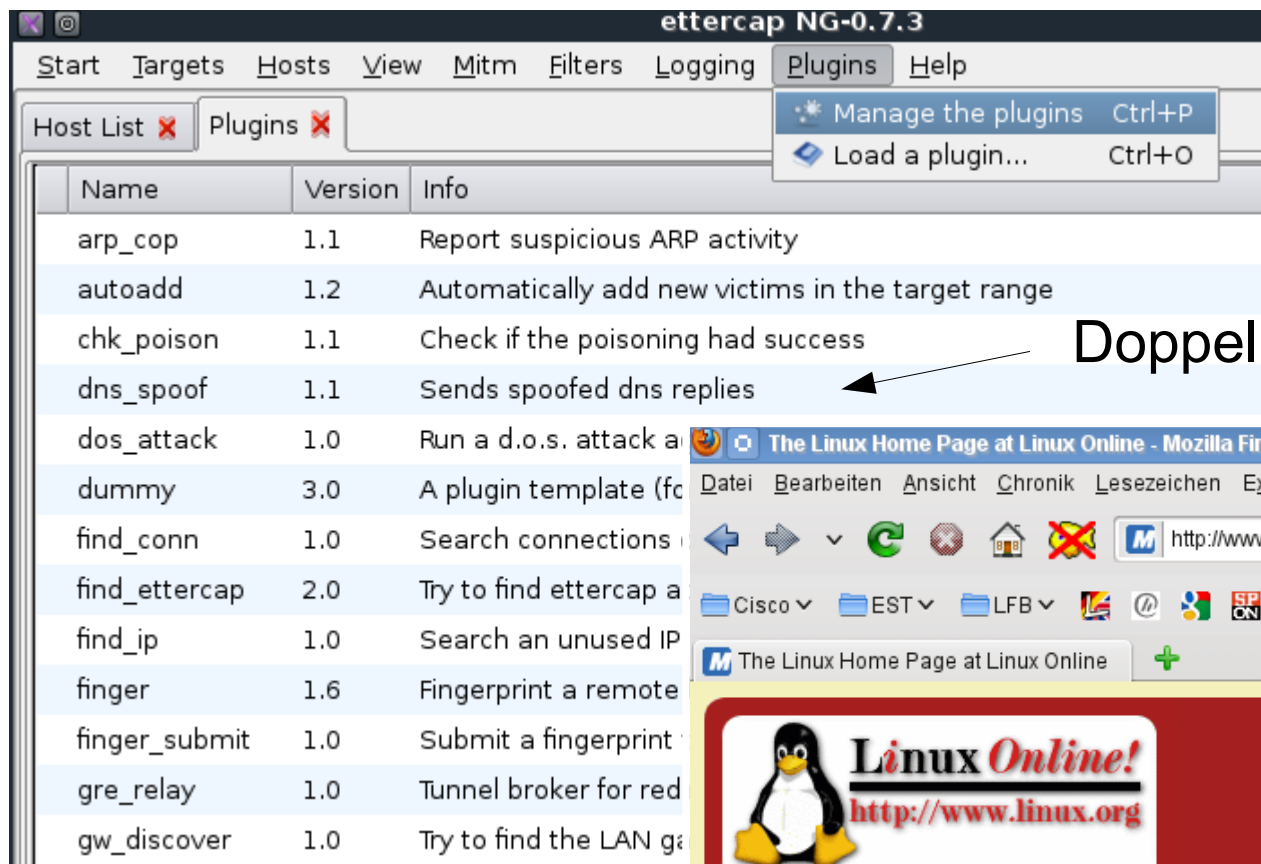
Noch! :-)

```
<div class="tab-contentPart active">
  <form class="form-l form-login" name="loginForm" meth
    <input type="hidden" name="AREA" value="1" />
    <input type="hidden" name="EXT" value="redirect"
    <input type="hidden" name="EXT2" value="" />
    <input type="hidden" name="dlevel" value="c"/>
    <fieldset>
      <legend>Login</legend>
      <div class="form-item login-username">
        <input type="text" name="id" tabindex="1"
        <h:output class="status"></h:output>
        <span><a href="http://www.gmx.net/produkt
      </div>
      <div class="form-item login-password">
        <input type="password" name="p" tabindex=
        <h:output class="status"></h:output>
        <span><a
          href="http://service.gmx.net/de/cgi/g
          vergessen?</a></span>
      </div>
```

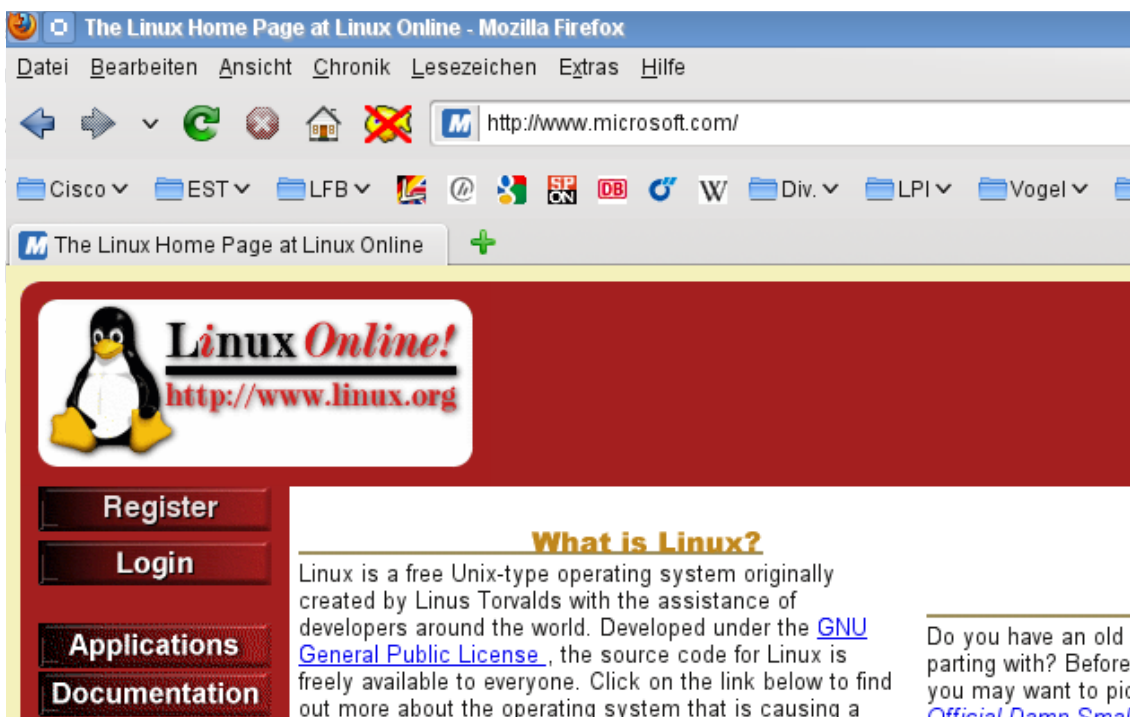
Nachpflegen interessanter Felder ...

- Beispiel für Login bei GMX:
Username → `id`
Passwort → `p`
- Eintragen der beiden Namen in
`/usr/share/ettercap/etter.fields`
im Abschnitt `[USER]` bzw. `[PASS]`

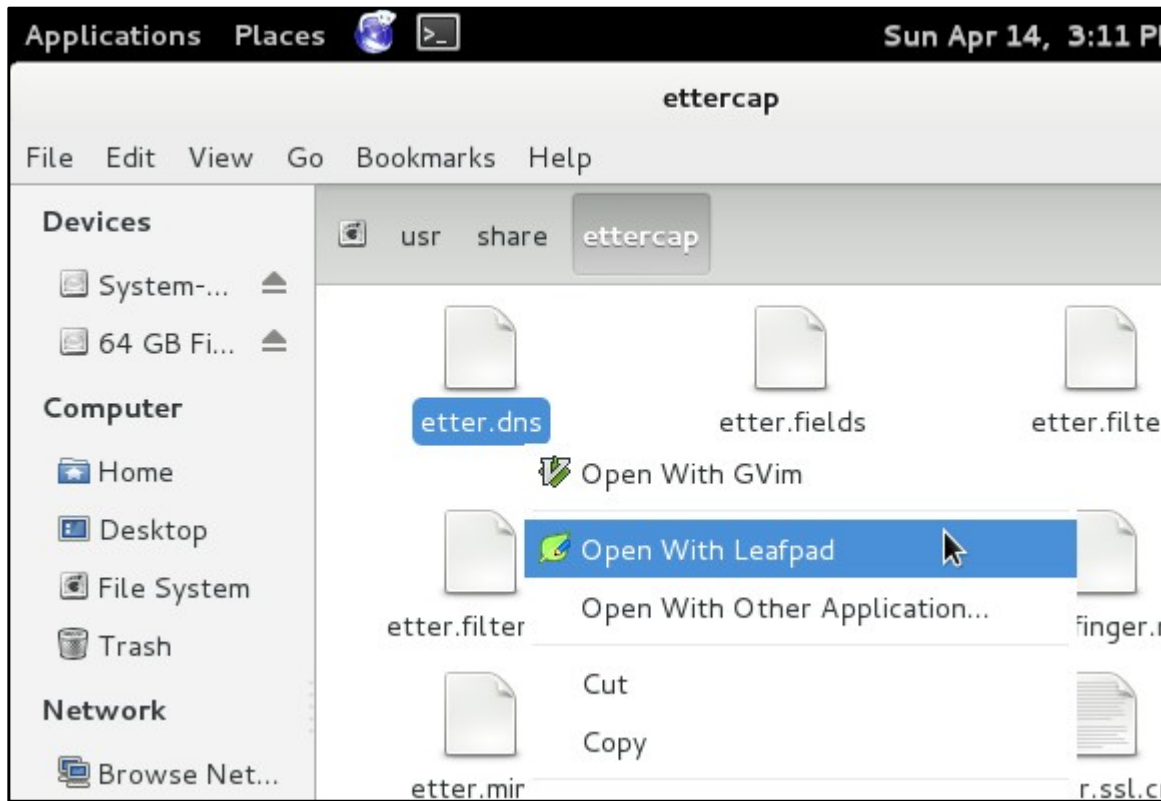
DNS-Spoofing - aktivieren



Doppelklick, ... ouups ...

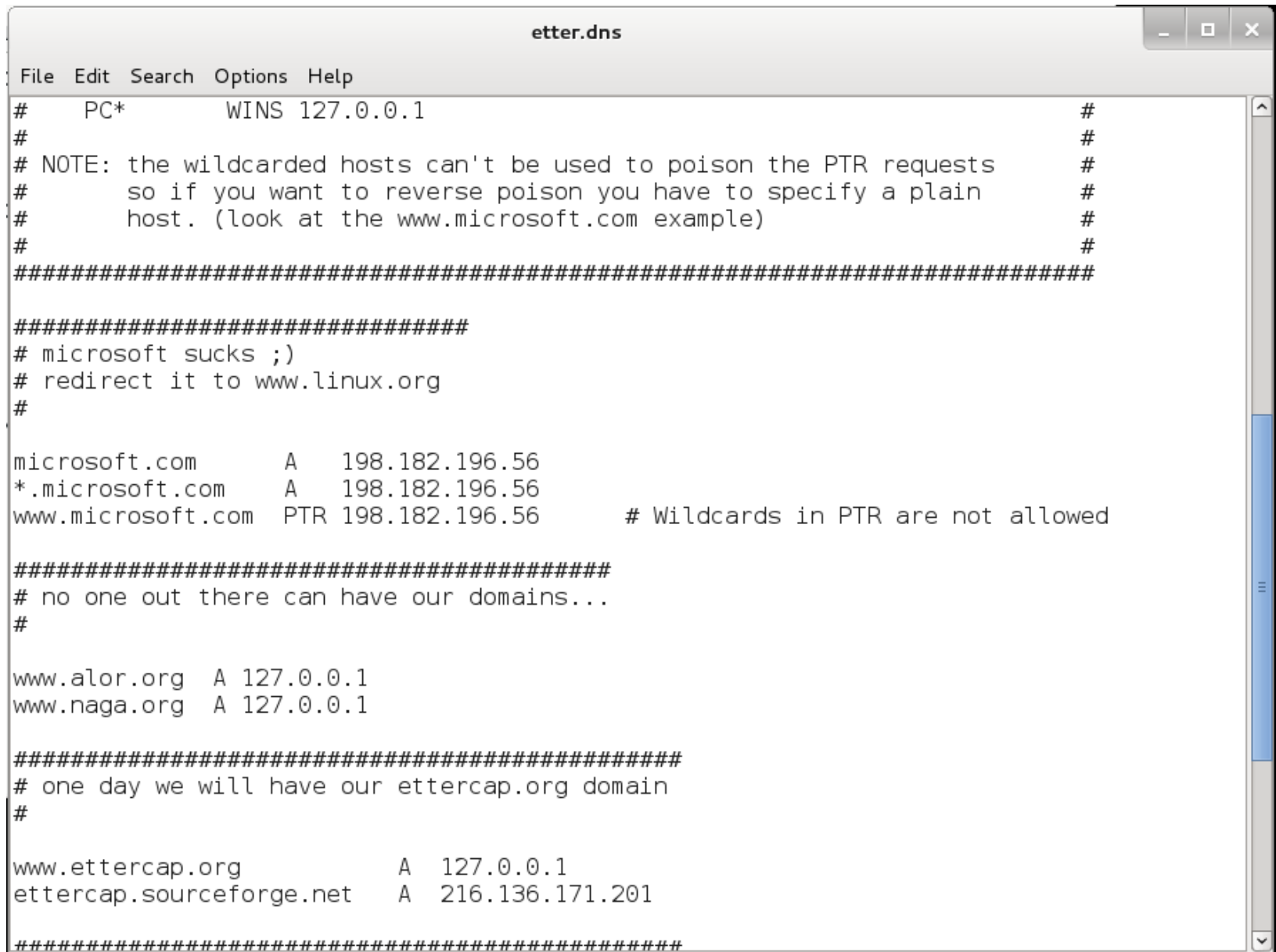


DNS-Spoofing – weitere Einträge ...



Doppelklick auf „Computer“ im Desktop → „File System“ → ins passende Verzeichnis durcklicken (/usr/share/ettercap) → rechter Mausklick auf „etter.dns“ → „Open With Leafpad“

DNS-Spoofing - ... einpflegen

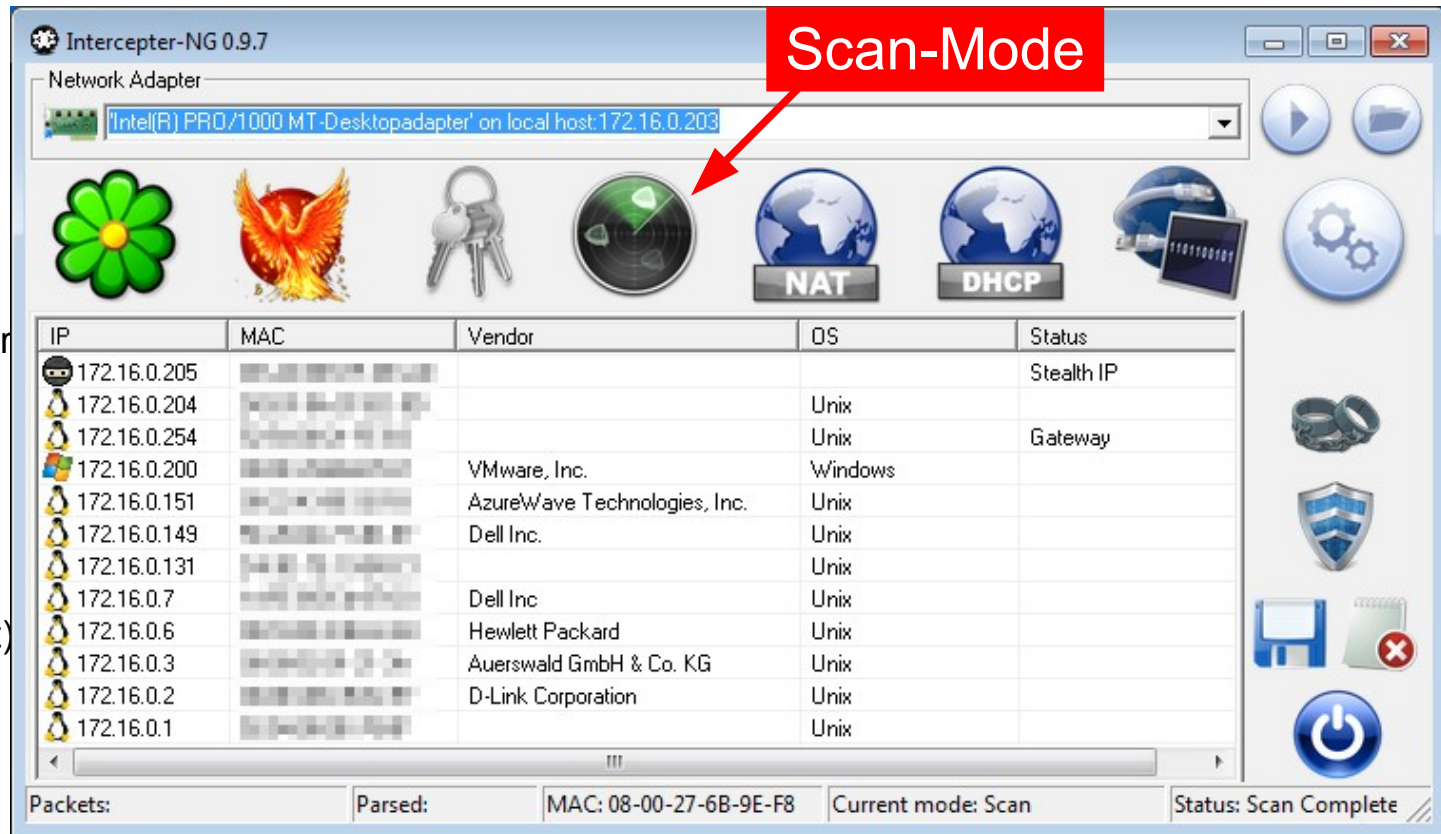
A screenshot of a window titled "etter.dns" with a standard menu bar (File, Edit, Search, Options, Help). The window contains a text editor with DNS spoofing configuration rules. The rules include a PC* entry for 127.0.0.1, a note about wildcarded hosts, and several A and PTR records for microsoft.com, alor.org, naga.org, ettercap.org, and sourceforge.net, all pointing to 127.0.0.1 or 216.136.171.201. The text is formatted with comments and separators.

```
etter.dns
File Edit Search Options Help
# PC* WINS 127.0.0.1 #
# #
# NOTE: the wildcarded hosts can't be used to poison the PTR requests #
# so if you want to reverse poison you have to specify a plain #
# host. (look at the www.microsoft.com example) #
# #
#####
#####
# microsoft sucks ;)
# redirect it to www.linux.org
#
microsoft.com A 198.182.196.56
*.microsoft.com A 198.182.196.56
www.microsoft.com PTR 198.182.196.56 # Wildcards in PTR are not allowed
#####
# no one out there can have our domains...
#
www.alor.org A 127.0.0.1
www.naga.org A 127.0.0.1
#####
# one day we will have our ettercap.org domain
#
www.ettercap.org A 127.0.0.1
ettercap.sourceforge.net A 216.136.171.201
#####
```

Interceptor-NG – Windows

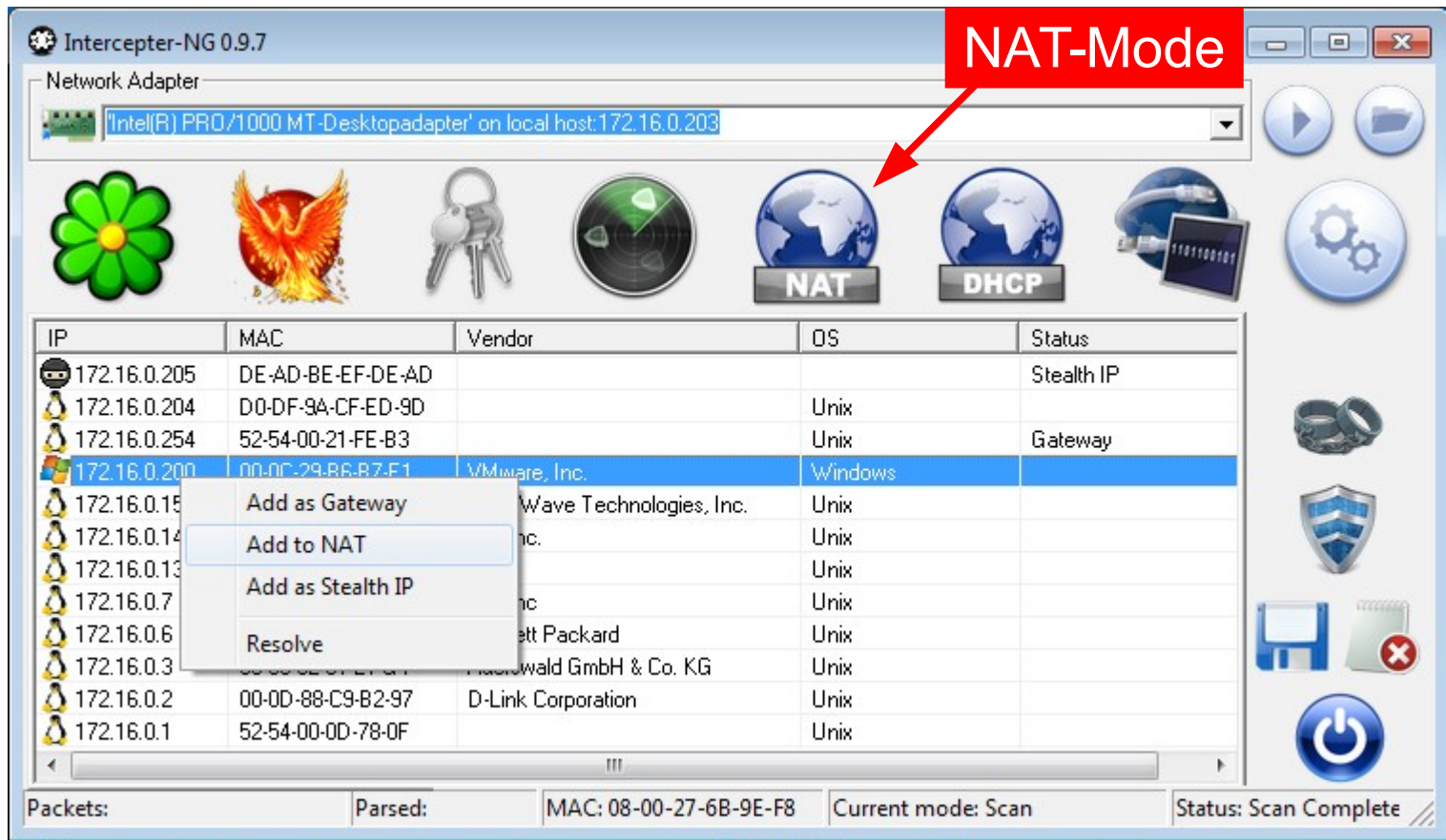
Features:

- x SSH MITM
- x PPPoE PAP Auth
- x NBNS\LLMNR Spoofing
- x Replaying sniffed cookies in browser
- x PCAP Over IP
- x SSLStrip: Cookie Killer
- x DNS Spoofing
- x MRA MD5 Auth
- x HTTP Auth Heur
- x Multiselecting of captures
- x Support of pcapng (new wireshark format)
- x Expert Mode
- x ARP Cage
- x IPv6 support
- x http injection
- x SMBRelay MiTM with NTLMv2 support
- ...



Nach dem Start zuerst richtiges Interface auswählen ...
dann im Scan-Mode → rechte Maustaste → Smart Scan

Interceptor-NG – Windows

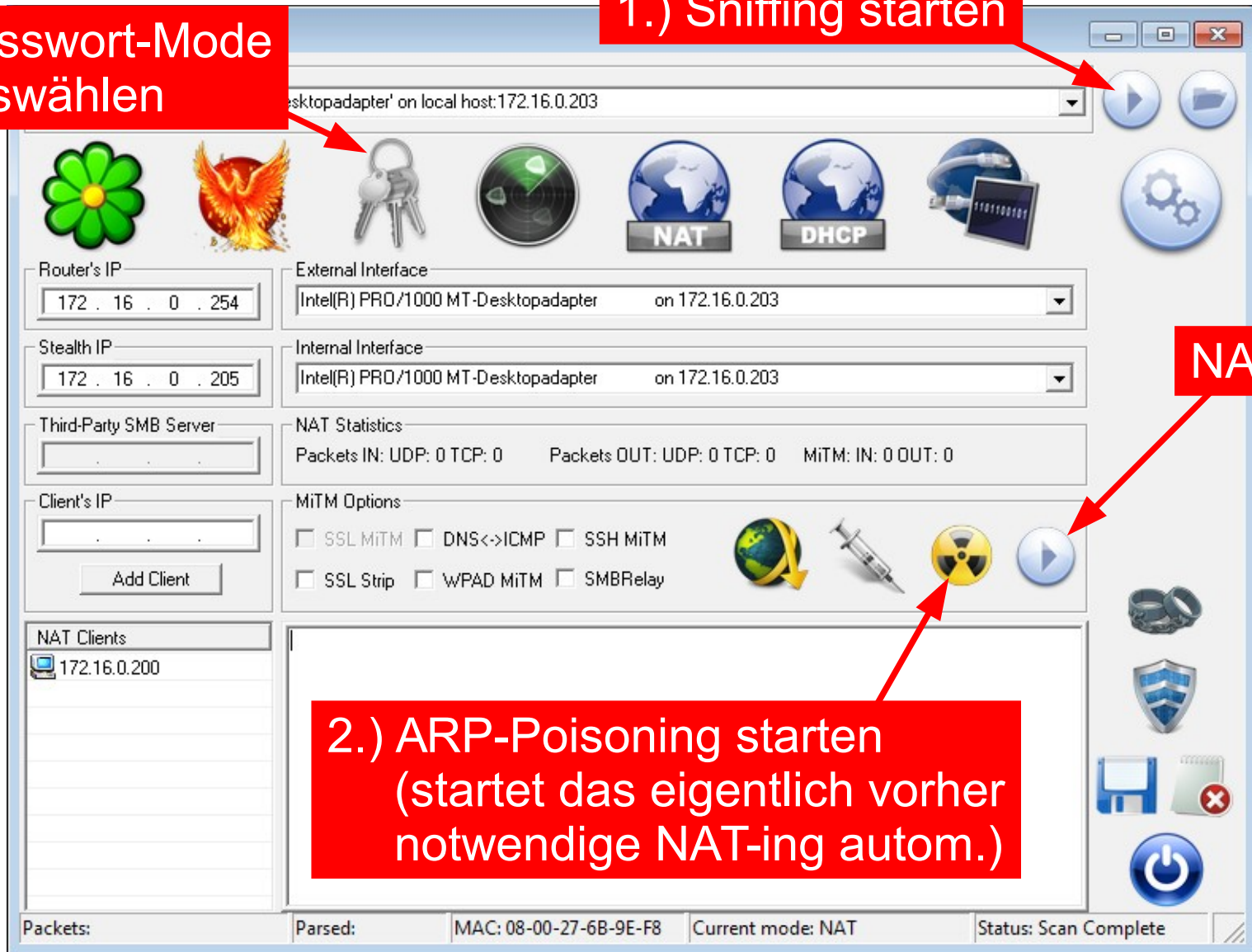


Zu spoofendes Opfer mit rechter Maustaste anklicken → „Add to NAT auswählen → auf NAT-Mode umschalten

Interceptor-NG – Windows

3.) Passwort-Mode auswählen

1.) Sniffing starten



Interceptor-NG – Windows

Interceptor-NG 0.9.7

Network Adapter

Intel(R) PRO/1000 MT-Desktopadapter' on local host:172.16.0.203

Icons: Flower, Phoenix, Keys, Green Circle, NAT, DHCP, Network Card

| Protocol | Time/Date | To/From | Host | Username | Password |
|----------------|-------------|---------------------|-------------------------|--------------|------------|
| WWW Basic A... | 17:29:34... | 217.24.203.146:8... | lehrerfortbildung-bw... | schlauberger | ganzgeheim |

„Opfer“ hat sich per http angemeldet!

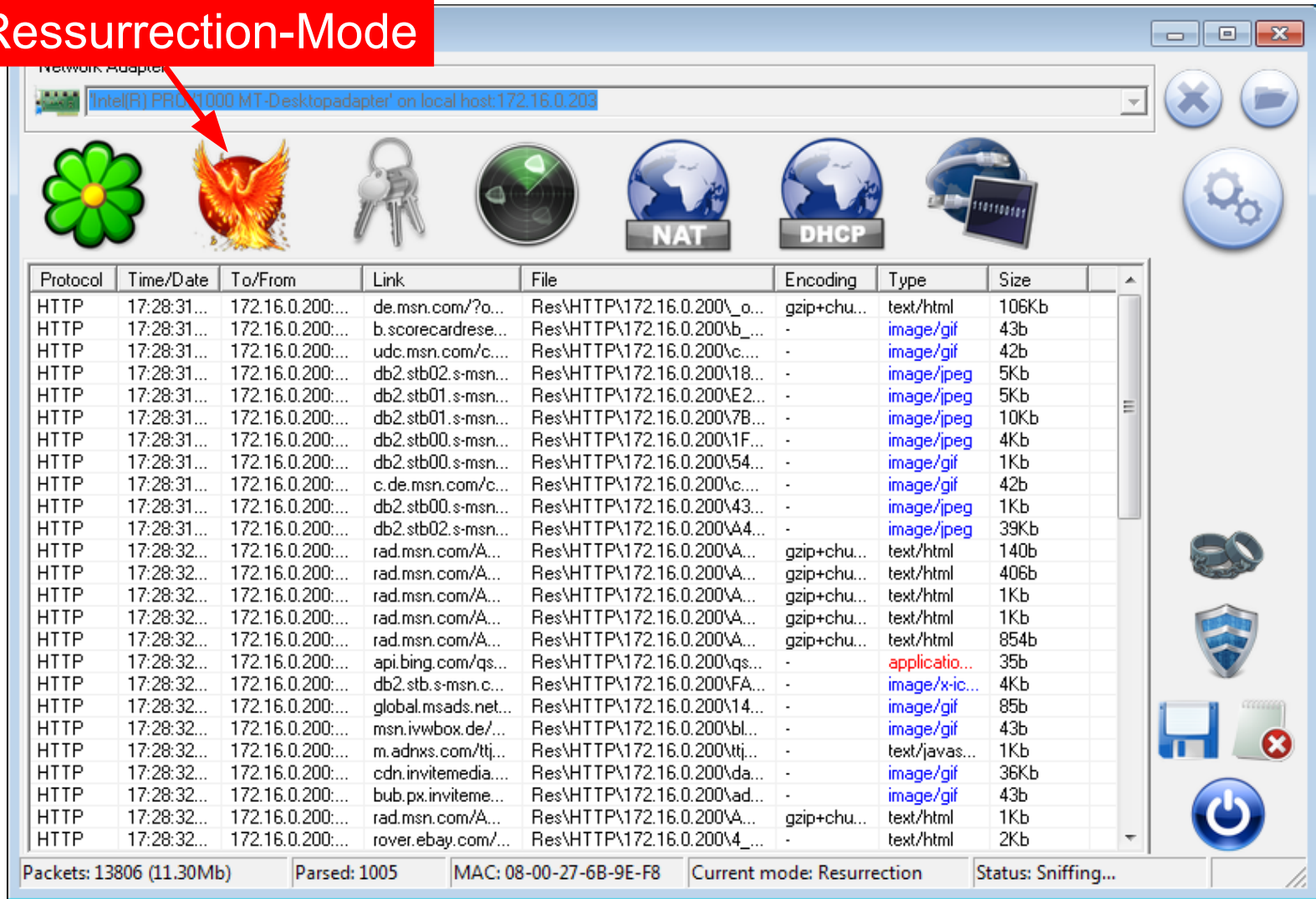
Fazit: So meldet man sich NIE an!

SSL- und SSH-Man-in-the-middle machen wir später :-)

Packets: 8649 (7.64Mb) | Parsed: 631 | MAC: 08-00-27-6B-9E-F8 | Current mode: Password | Status: Sniffing...

Interceptor-NG – Windows

Ressurrection-Mode



The screenshot shows the Interceptor-NG application window. At the top, a red banner reads 'Ressurrection-Mode'. Below it, a network adapter dropdown menu is visible, showing 'Intel(R) PRO/1000 MT-Desktopadapter' on local host: 172.16.0.203. A red arrow points to the 'Ressurrection-Mode' button, which is a phoenix icon. The interface includes a toolbar with various icons, including a green flower, a phoenix, a key, a globe, a NAT button, a DHCP button, and a power button. Below the toolbar is a table of intercepted traffic. The table has columns for Protocol, Time/Date, To/From, Link, File, Encoding, Type, and Size. The status bar at the bottom shows 'Packets: 13806 (11.30Mb)', 'Parsed: 1005', 'MAC: 08-00-27-6B-9E-F8', 'Current mode: Resurrection', and 'Status: Sniffing...'.

| Protocol | Time/Date | To/From | Link | File | Encoding | Type | Size |
|----------|-------------|-----------------|---------------------|------------------------------|-------------|---------------|-------|
| HTTP | 17:28:31... | 172.16.0.200... | de.msn.com/?o... | Res\HTTP\172.16.0.200\o... | gzip+chu... | text/html | 106Kb |
| HTTP | 17:28:31... | 172.16.0.200... | b.scorecardrese... | Res\HTTP\172.16.0.200\b... | - | image/gif | 43b |
| HTTP | 17:28:31... | 172.16.0.200... | udc.msn.com/c... | Res\HTTP\172.16.0.200\c... | - | image/gif | 42b |
| HTTP | 17:28:31... | 172.16.0.200... | db2.stb02.s-msn... | Res\HTTP\172.16.0.200\18... | - | image/jpeg | 5Kb |
| HTTP | 17:28:31... | 172.16.0.200... | db2.stb01.s-msn... | Res\HTTP\172.16.0.200\E2... | - | image/jpeg | 5Kb |
| HTTP | 17:28:31... | 172.16.0.200... | db2.stb01.s-msn... | Res\HTTP\172.16.0.200\7B... | - | image/jpeg | 10Kb |
| HTTP | 17:28:31... | 172.16.0.200... | db2.stb00.s-msn... | Res\HTTP\172.16.0.200\1F... | - | image/jpeg | 4Kb |
| HTTP | 17:28:31... | 172.16.0.200... | db2.stb00.s-msn... | Res\HTTP\172.16.0.200\54... | - | image/gif | 1Kb |
| HTTP | 17:28:31... | 172.16.0.200... | c.de.msn.com/c... | Res\HTTP\172.16.0.200\c... | - | image/gif | 42b |
| HTTP | 17:28:31... | 172.16.0.200... | db2.stb00.s-msn... | Res\HTTP\172.16.0.200\43... | - | image/jpeg | 1Kb |
| HTTP | 17:28:31... | 172.16.0.200... | db2.stb02.s-msn... | Res\HTTP\172.16.0.200\A4... | - | image/jpeg | 39Kb |
| HTTP | 17:28:32... | 172.16.0.200... | rad.msn.com/A... | Res\HTTP\172.16.0.200\A... | gzip+chu... | text/html | 140b |
| HTTP | 17:28:32... | 172.16.0.200... | rad.msn.com/A... | Res\HTTP\172.16.0.200\A... | gzip+chu... | text/html | 406b |
| HTTP | 17:28:32... | 172.16.0.200... | rad.msn.com/A... | Res\HTTP\172.16.0.200\A... | gzip+chu... | text/html | 1Kb |
| HTTP | 17:28:32... | 172.16.0.200... | rad.msn.com/A... | Res\HTTP\172.16.0.200\A... | gzip+chu... | text/html | 1Kb |
| HTTP | 17:28:32... | 172.16.0.200... | rad.msn.com/A... | Res\HTTP\172.16.0.200\A... | gzip+chu... | text/html | 854b |
| HTTP | 17:28:32... | 172.16.0.200... | api.bing.com/qs... | Res\HTTP\172.16.0.200\qs... | - | applicatio... | 35b |
| HTTP | 17:28:32... | 172.16.0.200... | db2.stb.s-msn.c... | Res\HTTP\172.16.0.200\FA... | - | image/x-ic... | 4Kb |
| HTTP | 17:28:32... | 172.16.0.200... | global.msads.net... | Res\HTTP\172.16.0.200\14... | - | image/gif | 85b |
| HTTP | 17:28:32... | 172.16.0.200... | msn.ivwbox.de/... | Res\HTTP\172.16.0.200\bl... | - | image/gif | 43b |
| HTTP | 17:28:32... | 172.16.0.200... | m.adnxs.com/tj... | Res\HTTP\172.16.0.200\itj... | - | text/javas... | 1Kb |
| HTTP | 17:28:32... | 172.16.0.200... | cdn.invitemedia... | Res\HTTP\172.16.0.200\da... | - | image/gif | 36Kb |
| HTTP | 17:28:32... | 172.16.0.200... | bub.px.inviteme... | Res\HTTP\172.16.0.200\ad... | - | image/gif | 43b |
| HTTP | 17:28:32... | 172.16.0.200... | rad.msn.com/A... | Res\HTTP\172.16.0.200\A... | gzip+chu... | text/html | 1Kb |
| HTTP | 17:28:32... | 172.16.0.200... | rover.ebay.com/... | Res\HTTP\172.16.0.200\4... | - | text/html | 2Kb |

Packets: 13806 (11.30Mb) Parsed: 1005 MAC: 08-00-27-6B-9E-F8 Current mode: Resurrection Status: Sniffing...

Im Ressurrection-Mode können wir das mitgeschnittene später in Ruhe ansehen :-)

Interceptor-NG – Windows

Interceptor-NG 0.9.7

Network Adapter: Intel(R) PRO/1000 MT-Desktopadapter on local host: 172.16.0.203

RAW-Mode

Icons: Flower, Phoenix, Keys, Radar, NAT, DHCP, Network Adapter (highlighted), Settings, Firewall, Shield, Disk, Power.

| No | Time | Source | Destination | Protocol | Len | Info |
|----|----------|-------------------|-------------------|----------|------|-------------------------------|
| 49 | 3.409206 | 172.16.0.131 | 172.16.0.1 | TCP | 1180 | 943 > 2049 Data |
| 50 | 3.409310 | 172.16.0.1 | 172.16.0.131 | TCP | 0 | [ACK] |
| 51 | 3.499048 | 172.16.0.1 | 172.16.0.131 | TCP | 140 | 2049 > 943 Data |
| 52 | 3.499051 | 172.16.0.131 | 172.16.0.1 | TCP | 0 | [ACK] |
| 53 | 4.30887 | 00-19-99-AE-82-EB | FF-FF-FF-FF-FF-FF | ARP | 0 | Request: who has 172.16.0.11? |
| 54 | 4.778212 | 172.16.0.131 | 172.16.0.1 | TCP | 120 | 943 > 2049 Data |
| 55 | 4.778516 | 172.16.0.1 | 172.16.0.131 | TCP | 124 | 2049 > 943 Data |
| 56 | 4.778518 | 172.16.0.131 | 172.16.0.1 | TCP | 0 | [ACK] |

Src: D4-3D-7E-19-B0-C1, Dst: 52-54-00-0D-78-0F, 186 bytes on wire
Src: 172.16.0.131, Dst: 172.16.0.1
TCP Src: 943, Dst: 2049

| Offset | Hex | ASCII |
|--------|---|-------------------------------------|
| 01 | 80 00 00 74 3D 74 70 C1 00 00 00 00 00 00 00 02 | €..t=tpÁ..... |
| 02 | 00 01 86 A3 00 00 00 03 00 00 00 04 00 00 00 01 | ..t&..... |
| 03 | 00 00 00 28 00 41 8E C6 00 00 00 09 72 2D 61 6E | ...(.AŽE....r-an |
| 04 | 64 72 65 61 73 00 00 00 00 00 03 E8 00 00 00 64 | dreas.....è...d |
| 05 | 00 00 00 02 00 00 00 64 00 00 00 70 00 00 00 00 |d...p.... |
| 06 | 00 00 00 00 00 00 00 1C 01 00 06 01 76 BF 45 91 |v&E' |
| 07 | 38 2D 40 81 88 3F B3 B6 35 2B 80 CF 01 00 F2 00 | 88 3F B3 B6 35 2B 80 CF 01 00 F2 00 |

Pcap Filter:

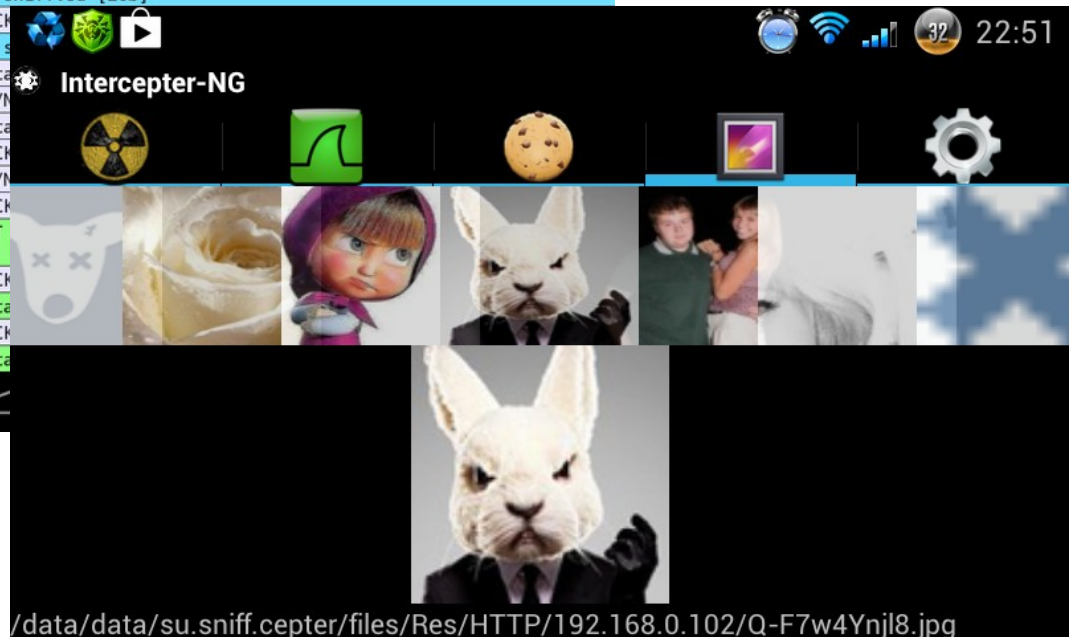
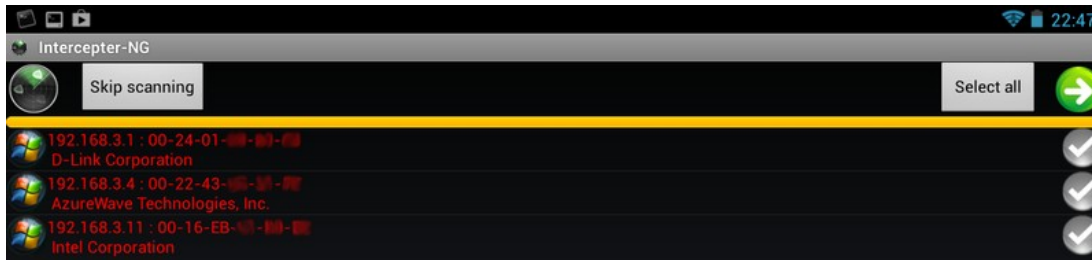
Stream Filter:

Packets: 14565 (11.62Mb) | Parsed: 1536 | MAC: 08-00-27-6B-9E-F8 | Current mode: RAW | Status: Sniffing...

Packet-Capturing im RAW-Mode à la Wireshark! Speicherbar!!!

Interceptor-NG – Android

Quelle:
Wiki von Interceptor



XArp – Abwehr für Windows u. Linux

XArp - unregistered version

File XArp Professional Help

✓ Status: no ARP attacks Security level set to: basic

- View detected attacks
- Read the 'Handling ARP attacks' help
- View XArp logfile

Get XArp Professional now!
Register XArp Professional

aggressive
high
basic
minimal

| | IP | MAC | Host | Vendor | Interface | Onli |
|---|--------------|-----|---------------------|-------------------|---------------------|----------|
| ✓ | 172.16.0.1 | | server.grupp.p... | Realtek (uptec... | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.2 | | 172.16.0.2 | D-link Corpora... | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.3 | | 172.16.0.3 | Auerswald Gm... | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.6 | | procurve.grupp... | Hewlett Packard | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.7 | | dellserv.grupp... | unknown | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.131 | | 172.16.0.131 | Fujitsu Siemen... | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.149 | | r-laptop5.grup... | unknown | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.219 | | 172.16.0.219 | Fujitsu Techno... | 0xb - Intel(R) P... | unkn |
| ✓ | 172.16.0.222 | | 172.16.0.222 | Cisco-linksys Llc | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.223 | | Test-VM.grup... | Cadmus Com... | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.254 | | ipfire.grupp.pri... | Realtek (uptec... | 0xb - Intel(R) P... | unkno... |

XArp 2.2.2

Advanced ARP spoofing detection

©2004-2011 - Christoph P. Mayer - All rights reserved.
www.chrismc.de xarp@chrismc.de

Registered to: <unregistered>

Credits Close

XArp 2.2.2 - 11 mappings - 1 interface - 0 alerts

XArp nach ARP-Spoofing-Angriff

XArp - unregistered version
File XArp Professional Help

Status: ARP attacks detected! Security level set to: basic

- View detected attacks
- Read the 'Handling ARP attacks' help
- View XArp logfile

[Get XArp Professional now!](#)
[Register XArp Professional](#)

Security level options: aggressive, high, **basic**, minimal

The basic security level operates a default attack detection strategy that can detect all standard attacks. This is the suggested level for default environments.

| | IP | MAC | Host | Vendor | Interface | Online |
|---|--------------|-------------------|---------------------|-------------------|---------------------|----------|
| ✗ | 172.16.0.1 | 00-0c-29-9a-79-b3 | server.grupp.p... | Realtek (uptec... | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.2 | 08-00-27-f4-ff-55 | 172.16.0.2 | D-link Corpora... | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.3 | 08-00-27-f4-ff-55 | 172.16.0.3 | Auerswald Gm... | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.6 | 08-00-27-f4-ff-55 | 172.16.0.6 | Hewlett Packard | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.7 | 08-00-27-f4-ff-55 | dellserv.grupp... | unknown | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.131 | 08-00-27-f4-ff-55 | 172.16.0.131 | Fujitsu Siemen... | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.149 | 08-00-27-f4-ff-55 | r-laptop5.grup... | unknown | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.219 | 08-00-27-f4-ff-55 | 172.16.0.219 | Fujitsu Techno... | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.222 | 08-00-27-f4-ff-55 | 172.16.0.222 | Cisco-linksys Llc | 0xb - Intel(R) P... | unkno... |
| ✗ | 172.16.0.223 | 08-00-27-f4-ff-55 | Test-VM.grup... | Cadmus Com... | 0xb - Intel(R) P... | unkno... |
| ✗ | 172.16.0.224 | 00-0c-29-9a-79-b3 | 172.16.0.224 | Vmware, Inc. | 0xb - Intel(R) P... | unkno... |
| ✓ | 172.16.0.254 | 08-00-27-f4-ff-55 | ipfire.grupp.pri... | Realtek (uptec... | 0xb - Intel(R) P... | unkno... |

XArp 2.2.2 - 12 mappings - 1 interface - 12 alerts

Alert 8 of 12 16:30:11

ChangeFilter: MAC address for IP 172.16.0.1 changed from 52-54-00-0d-78-0f to 00-0c-29-9a-79-b3

Interface : 0xb
[ethernet]
source mac : 00-0c-29-9a-79-b3
dest mac : 08-00-27-f4-ff-55
type : 0x806
[arp]
direction : in
type : reply
source ip : 172.16.0.1
dest ip : 172.16.0.223
source mac : 00-0c-29-9a-79-b3
dest mac : 08-00-27-f4-ff-55

Arpwatch – sendet bei Angriffen Mails



Lernen neuer
MAC-Adressen



Mails nach
potentiellem Angriff



Android – z.B. DroidSheep-Guard

<http://droidsheep.de/>



DROIDSHEEP

Weitere Verteidigungs-Möglichkeiten

- Kostenpflichtige Lösungen
 - von „Arpwatch“ in einer Appliance
 - bis zu extrem mächtigen Appliances (Sensoren im Netz, Reporting, ...)
- Direkt „vor Ort“ an der Angriffsquelle
→ im Layer-2-Switch
 - Port Security
 - BPDU-Guard, Root-Guard
 - Storm-Control
 - DHCP-Snooping
 - Dynamic ARP Inspection (DAI)