

Das ist aber spoofy ...

Tom Gries (TOMO) | September 2023



@tomo@chaos.social



2023-09-02

Legal Disclaimer - Hackerparagraf

Die hier vorgestellten Methoden und Tools dienen zum Schutz der eigenen Systeme. Das Knacken fremder Passwörter ebenso wie das Eindringen in Systeme kann eine Straftat darstellen. Die vorgestellten Tools können unter den Hackerparagrafen 202c StGB fallen. Entsprechend dürfen Sie nur auf eigene Kennwörter oder Testsysteme losgehen, beziehungsweise sich schriftlich die Erlaubnis des Systembesitzers einholen.

Zudem können Cracking-Tools die getesteten Systeme stark beeinträchtigen oder außer Funktion setzen. Entsprechend vorsichtig sollten Sie bei Produktivsystemen sein.

Was versteht man eigentlich unter Spoofing?

Spoofing kann man mit schwindeln übersetzen. Damit ist das Fälschen von Angaben oder Identitäten gemeint. Spoofer geben sich für jemand anderen aus oder verwenden gefälschte Netzwerkbeziehungsweise Geräteadressen(MAC-Adressen, IP-Adressen, URLs). Spoofing ist im Allgemeinen die Vorbereitung auf ...

- ⇒ ... Phishing
- ⇒ ... Trojaner
- ⇒ ... Ransomware

Wesentlichen Spoofingarten sind:

- ⇒ ARP Spoofing
- ⇒ IP Spoofing
- ⇒ Caller-ID Spoofing
- ⇒ SMS-Spoofing
- ⇒ Public Key / PKI Spoofing
- ⇒ URL Spoofing
- ⇒ DNS Spoofing
- ⇒ Mail Spoofing



Eine typische URL ...

<http://www.facebook.com@678605212/#index.php?PageID=98332>



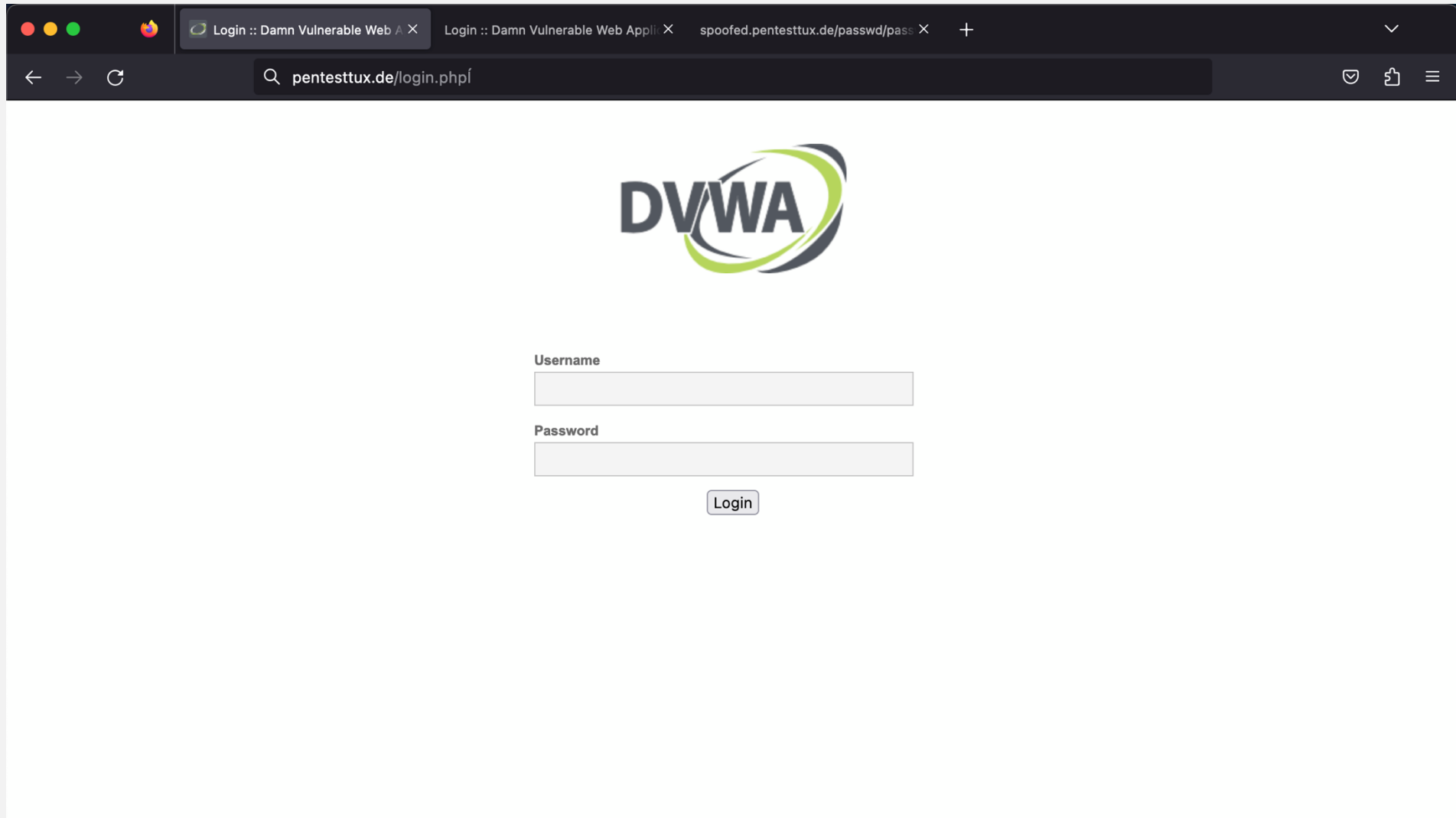
Spoofing Vorbereitung

Kopieren einer Website auf eigenen Server

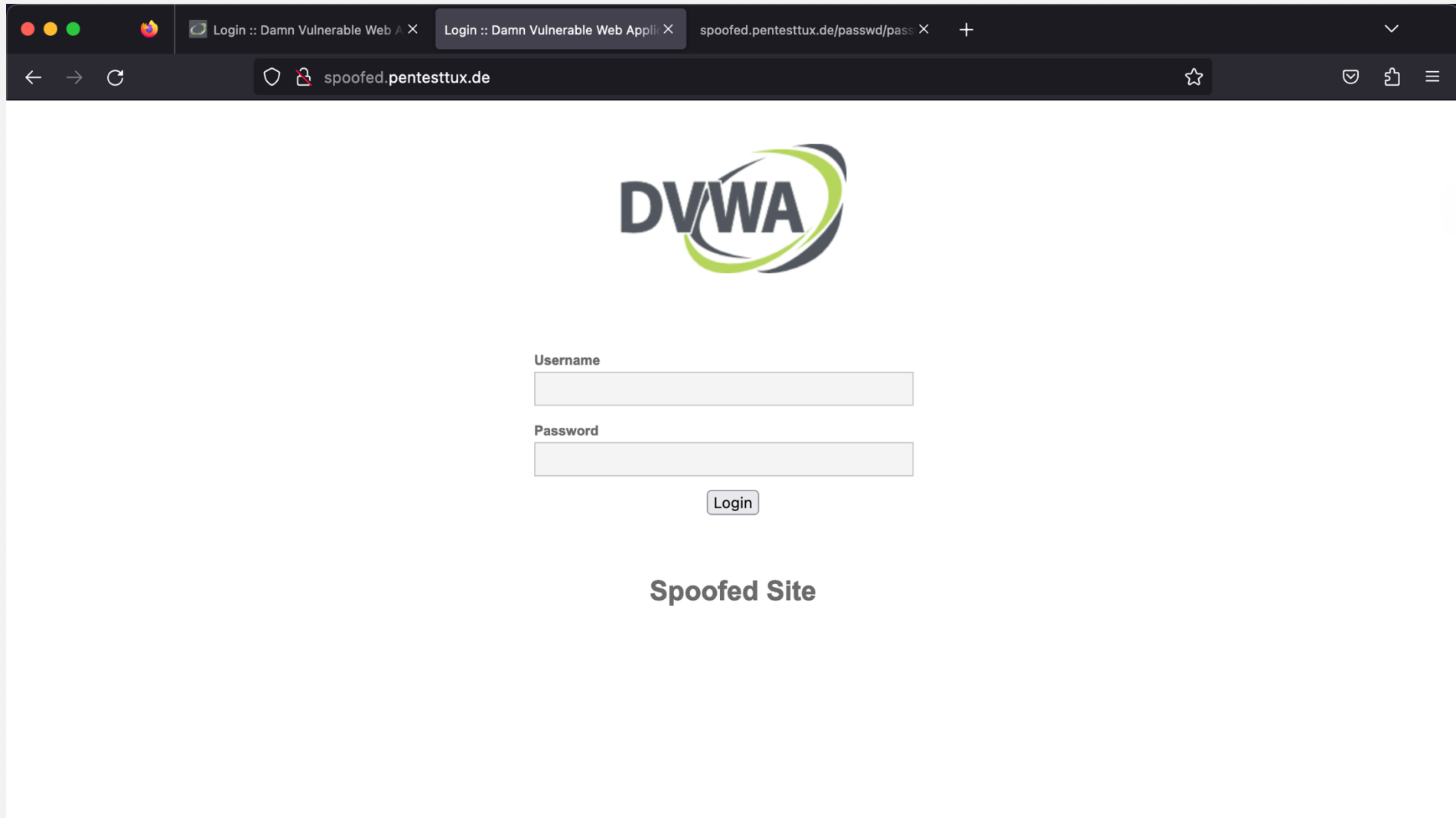
Der erste Schritt für URL und DNS Spoofing ist das Kopieren der Website, mit der der Angreifer das Opfer austricksen will. Das geht zum Beispiel mit `wget` (oder `WinWget` unter Windows).

Danach erfolgt eine Anpassung der HTML-Kopie. Eventuell fehlende Dateien (CSS, JS, Bilder etc.) werden manuell nachgeladen. Aus der HTML-Seite wird eine dynamische Seite (mit z. B. PHP) erstellt. Die Login-Felder werden überarbeitet (speichern der eingegebenen Daten) und es wird ein Redirect auf das Original implementiert.

Beispiel: Aus DVWA auf PENTESTTUX.DE ...



... wird SPOOFED.PENTESTTUX.DE



URL Spoofing (Verschleierung)

URL Spoofing (Verschleierung/Obfuscation)

<http://www.pentesttux.de@822940621/#index.php?PageID=98332>



DEMO

URL Spoofing (Verschleierung/Obfuscation)

`http://max:power@www.example.net:80/index.html?p1=A&p2=B#ressource`



Schema

Pfad

`http://www.dvwa.pentesttux.de@2391065710/#index.php?PageID=98332`

User

Host (in dezimal)

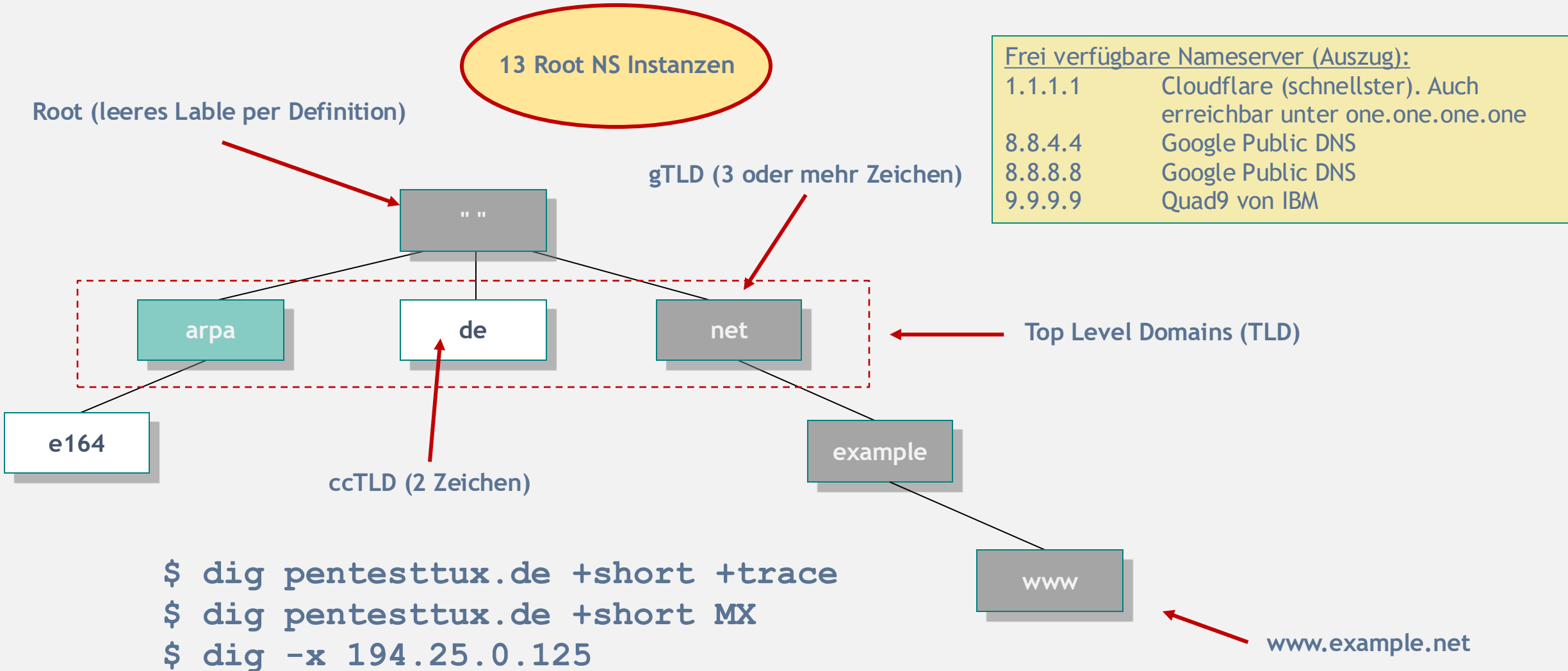
Fragment

RFC 3986

Hint: `ping 2391065710`

DNS Spoofing

Das DNS - Hierarchie

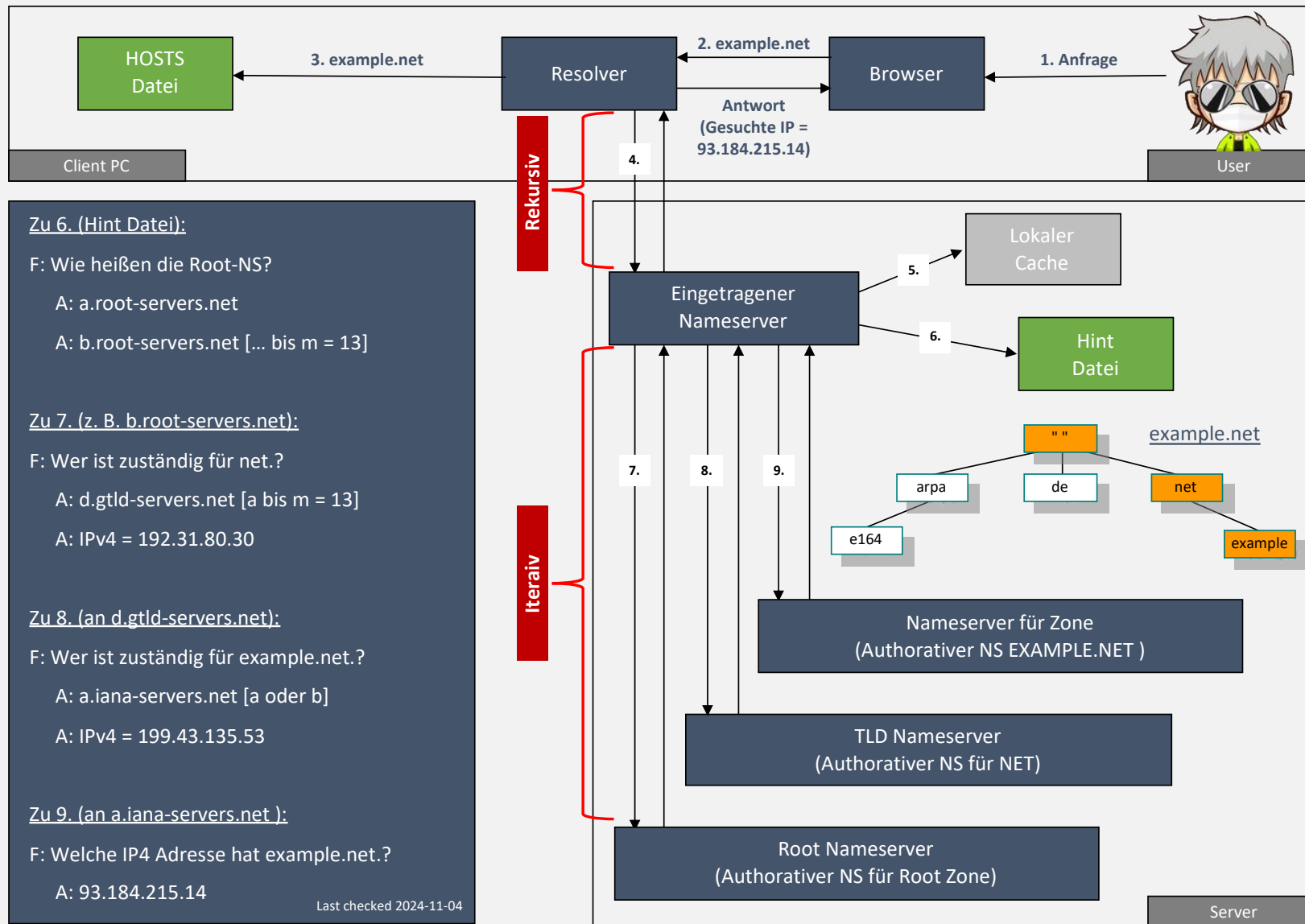


Das DNS - Adressierung im Nameserver

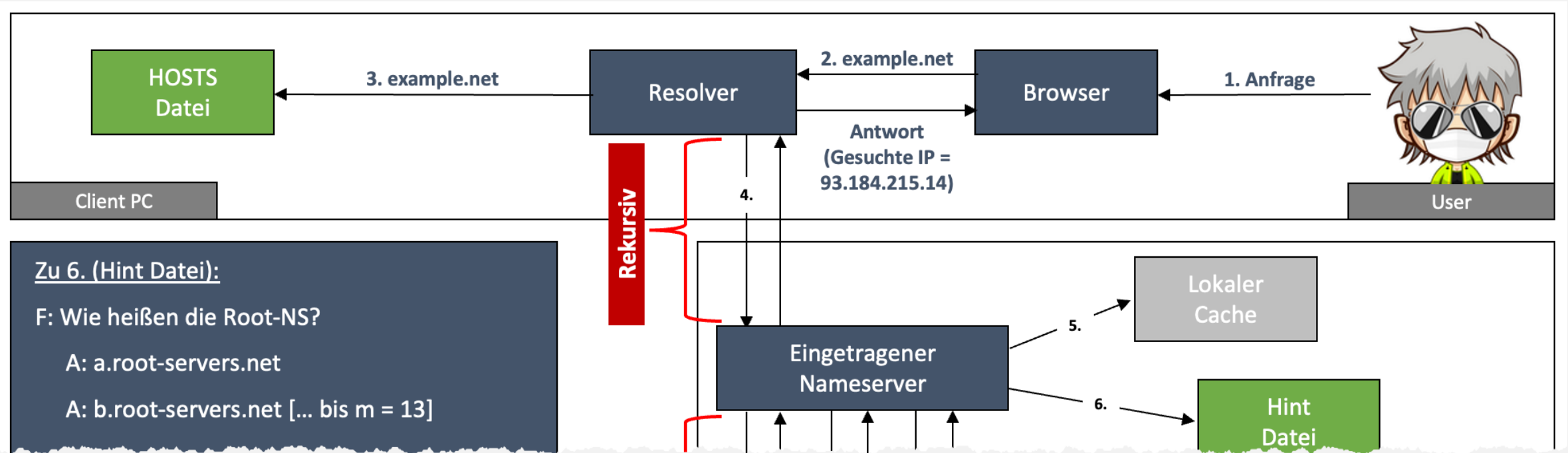
Beispiel einer Nameserver Zonendatei (BIND):

```
example.net. 1800 IN SOA ns1.example.net. mailbox.example.net. (  
    2021011701 ; Seriennummer  
    300        ; Refresh Time  
    100        ; Retry Time  
    6000       ; Expire Time  
    600        ; negative Caching Zeit  
    )  
example.net. 1800 IN NS ns1.example.net.  
www.example.net. 1800 IN A 192.168.1.2  
www.example.net. 1800 IN AAAA 2001:db8::1:2
```

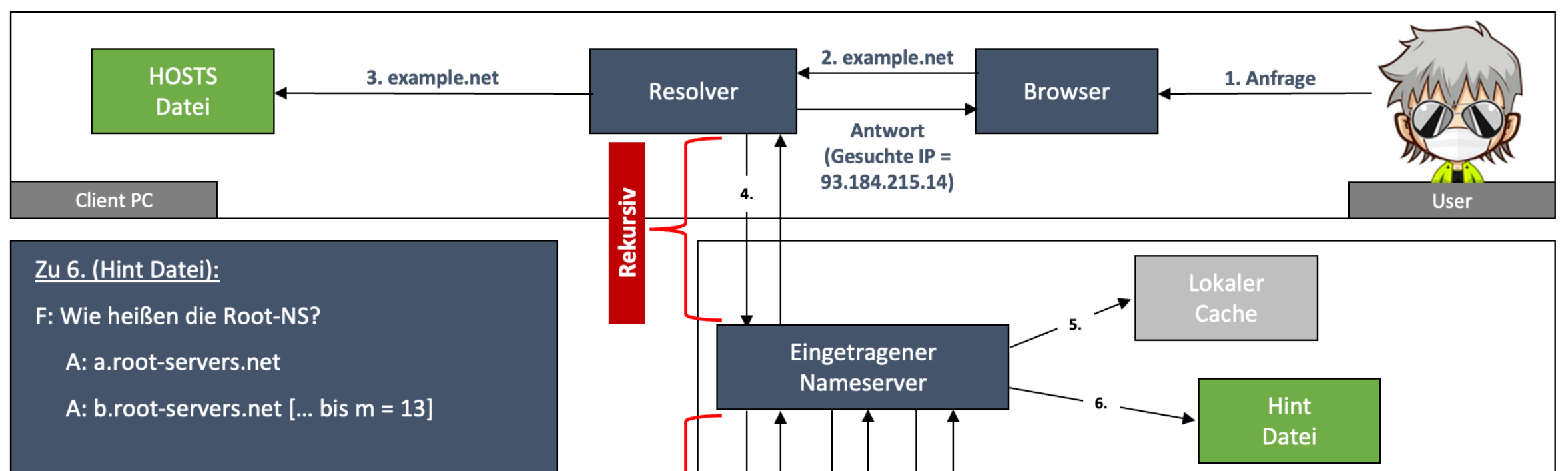
Das DNS - Namensauflösung



Das DNS - Namensauflösung



Das DNS - Namensauflösung



Das DNS - Spoofing mit lokaler HOSTS Datei

```
# This is a sample HOSTS file.  
#  
# This file is stored at C:\Windows\System32\drivers\etc\hosts  
# on Windows machines and at /etc/hosts on Linux/Unix machines.  
  
127.0.0.1          localhost localhorst horst  
127.127.10.80      web-server.local dev  
  
9.9.9.9            nine.nine.nine.nine nine quad-nine 4nine
```

Das DNS - Spoofing mit lokaler HOSTS Datei

```
# This is a sample HOSTS file.  
#  
# This file is stored at C:\Windows\System32\drivers\etc\hosts  
# on Windows machines and at /etc/hosts on Linux/Unix machines.  
  
127.0.0.1          localhost localhorst horst  
127.127.10.80      web-server.local dev  
  
9.9.9.9            nine.nine.nine.nine nine quad-nine 4nine  
  
### Example for IP-Spoofing  
40.114.177.156     example.net      ### IP of duckduckgo.com
```

Das DNS - Spoofing mit P4wnP1 A.L.O.A.

```
# This is a sample HOSTS file.  
#  
# This file is stored at C:\Windows\System32\drivers\etc\hosts  
# on Windows machines and at /etc/hosts on Linux/Unix machines.  
  
127.0.0.1          localhost localhorst horst  
127.127.10.80      web-server.local dev  
  
9.9.9.9            nine.nine.nine.nine nine quad-nine 4nine  
  
### set by P4wnP1 A.L.O.A.  
127.0.0.7          facebook.com www.facebook.com  
0.0.0.0            example.net www.example.net
```

Mail Spoofing

Telnet und SSH

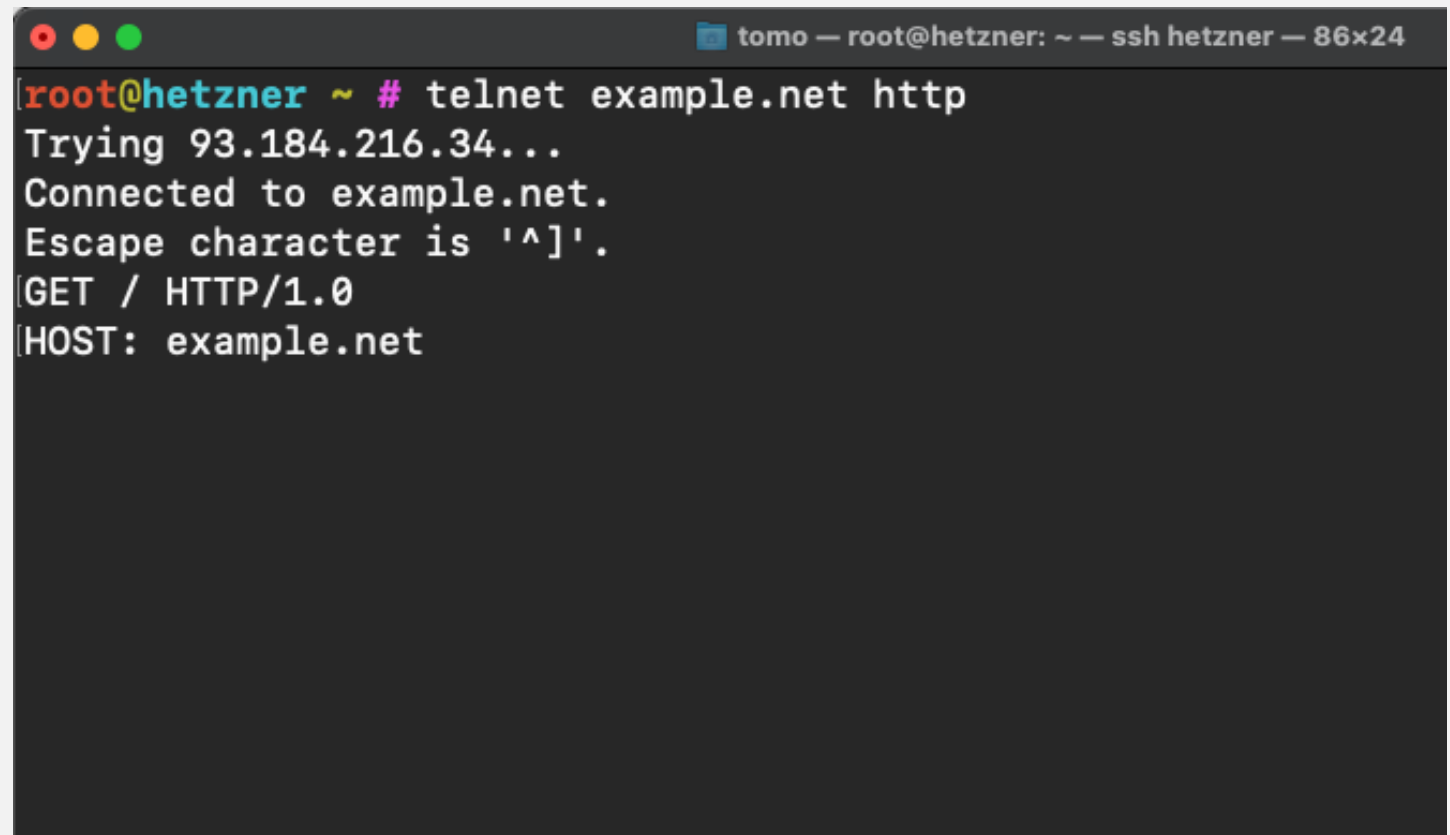
Telnet ist eins der ältesten Protokolle. Es wurde 1969 im Rahmen des ARPANET Projekts entwickelt, um Anwendungsprogramme und Datenbanken auch entfernt nutzen zu können. Telnet besteht aus einem Client, einem Server und dem Telnet Protokoll. Die Datenübertragung - auch vom Benutzernamen und Passwort - erfolgt unverschlüsselt. Telnet (der Client) wird heutzutage fast ausschließlich nur noch zur Fehlersuche und zur Ausbildung bei Klartextprotokollen verwendet.

SSH (Secure Shell) kann man als Nachfolger von Telnet betrachten. Die Verbindung inklusive dem Verbindungsaufbau ist verschlüsselt. Darüber hinaus bietet SSH noch weitere Funktionen, die Telnet nicht kannte (z. B. SCP) und dient als Basis für weitere Anwendungen (z. B. SFTP).

Telnet - der Client für Klartextprotokolle

Unter einem **Klartextprotokoll** versteht man ein Protokoll, das Daten mit dem Gegenüber unverschlüsselt - also im Klartext - austauscht. Das sind zum Beispiel:

- HTTP
- FTP
- SMTP
- POP3
- IMAP4
- Telnet selber
- und Weitere ...



```
tomo — root@hetzner: ~ — ssh hetzner — 86x24
root@hetzner ~ # telnet example.net http
Trying 93.184.216.34...
Connected to example.net.
Escape character is '^]'.
[GET / HTTP/1.0
[HOST: example.net
```


`telnet -6 towel.blinkenlights.nl`



Zuständigen Mailserver identifizieren

```
tomo — root@hetzner: ~ — ssh hetzner — 86x24
root@hetzner ~ # dig outlook.de MX

; <<>> DiG 9.16.42-Debian <<>> outlook.de MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37771
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;outlook.de.                IN      MX

;; ANSWER SECTION:
outlook.de.                2581    IN      MX      5 eur.olc.protection.outlook.com.

;; Query time: 0 msec
;; SERVER: 185.12.64.2#53(185.12.64.2)
;; WHEN: Sun Aug 13 19:21:40 UTC 2023
;; MSG SIZE  rcvd: 85

root@hetzner ~ #
```

Mail mit Telnet versenden

```
tomo — root@hetzner: ~ — ssh hetzner — 118x26
root@hetzner ~ # telnet eur.olc.protection.outlook.com smtp
Trying 104.47.14.33...
Connected to eur.olc.protection.outlook.com.
Escape character is '^]'.
220 VI1EUR04FT020.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Sun, 13 Aug 2023 20:02:35 +0000
HELO U
250 VI1EUR04FT020.mail.protection.outlook.com Hello [142.132.196.110]
MAIL FROM: <tom@pentesttux.de>
250 2.1.0 Sender OK
RCPT TO: <livehacking@outlook.de>
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: "Tom" <tom@pentesttux.de>
To: "LiveHacking" <livehacking@outlook.de>
Subject: Test vom Talk in Darmstadt (MRMCD)

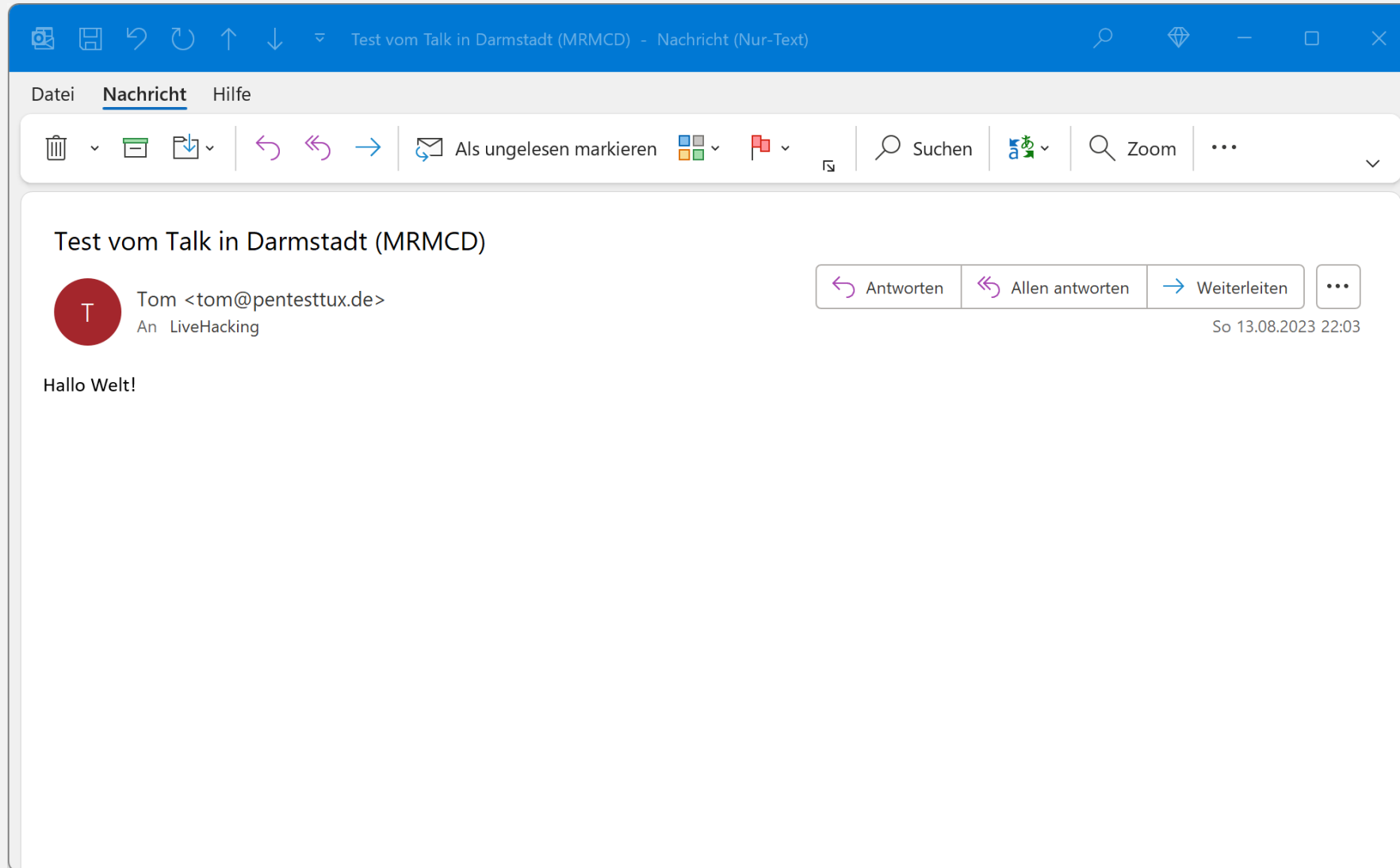
Hallo Welt!
.
250 2.6.0 <4cbcd10a-31ad-4e78-9731-4625d26040e0@VI1EUR04FT020.eop-eur04.prod.protection.outlook.com> [InternalId=47244
64026591, Hostname=AS4P195MB1814.EURP195.PROD.OUTLOOK.COM] 7706 bytes in 16.282, 0.462 KB/sec Queued mail for delivery
-> 250 2.1.5
QUIT
221 2.0.0 Service closing transmission channel
Connection closed by foreign host.
root@hetzner ~ #
```

Mail mit Telnet versenden

```
tomo — root@hetzner: ~ — ssh hetzner — 118x26
root@hetzner 1 telnet eur.olc.protection.outlook.com smtp
Trying 104.47.14.33...
Connected to eur.olc.protection.outlook.com.
Escape character is '^]'.
220 VI1EUR04FT020.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Sun, 13 Aug 2023 20:02:35 +0000
2 HELO U
250 VI1EUR04FT020.mail.protection.outlook.com Hello [142.132.196.110]
MAIL FROM: <tom@pentesttux.de>
250 2.1.0 Sender OK
3 RCPT TO: <livehacking@outlook.de>
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: "Tom" <tom@pentesttux.de>
To: "LiveHacking" <livehacking@outlook.de>
4 Subject: Test vom Talk in Darmstadt (MRMCD)

Hallo Welt!
.
250 2.6.0 <4cbcd10a-31ad-4e78-9731-4625d26040e0@VI1EUR04FT020.eop-eur04.prod.protection.outlook.com> [InternalId=47244
64026591, Hostname=AS4P195MB1814.EURP195.PROD.OUTLOOK.COM] 7706 bytes in 16.282, 0.462 KB/sec Queued mail for delivery
-> 250 2.1.5
QUIT
221 2.0.0 Service closing transmission channel
Connection closed by foreign host.
root@hetzner ~ #
```

Und so sieht es aus ...



Mail mit gefälschtem Absender

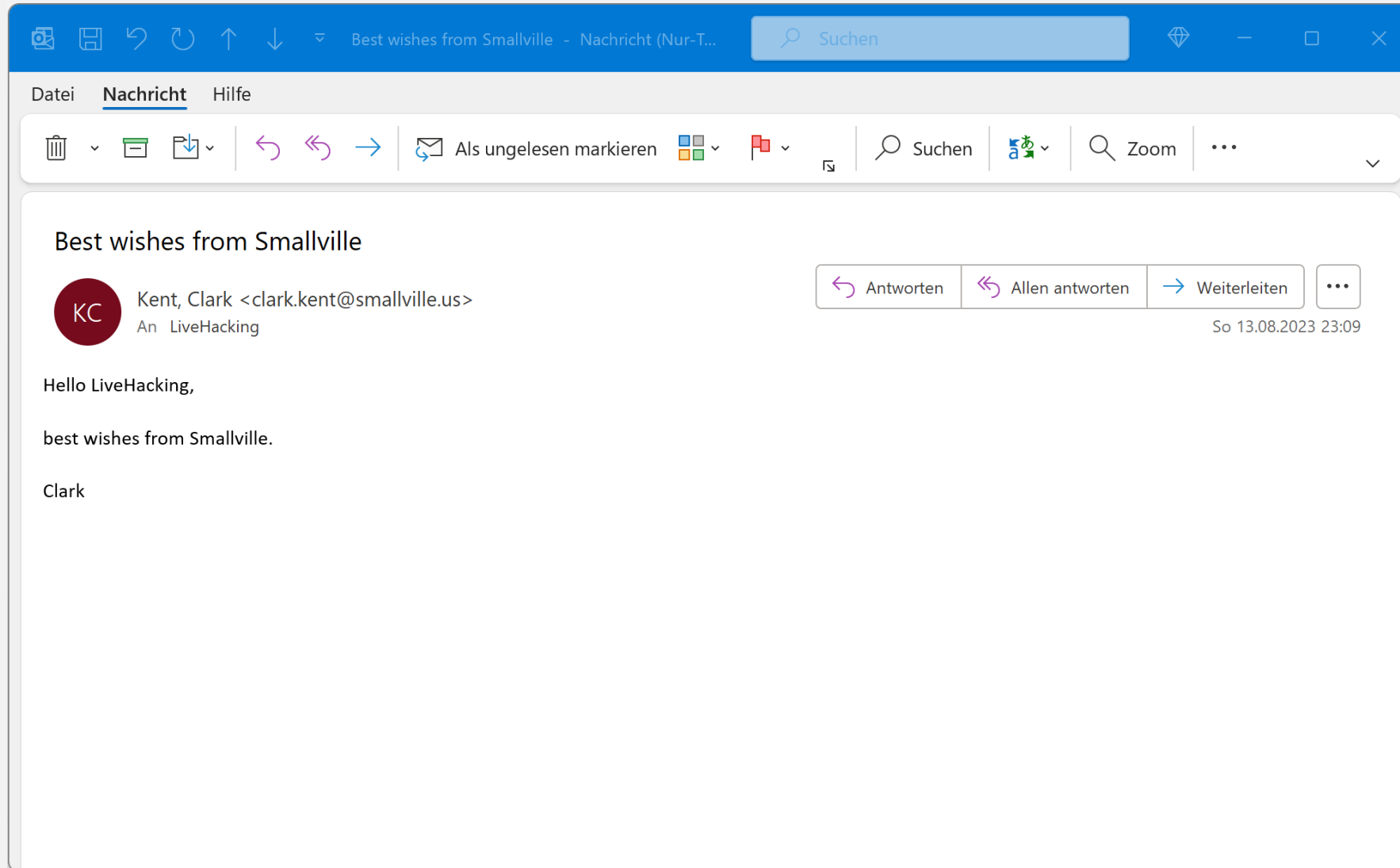
```
tomo — root@hetzner: ~ — ssh hetzner — 118x30
root@hetzner ~ # telnet eur.olc.protection.outlook.com smtp
Trying 104.47.18.225...
Connected to eur.olc.protection.outlook.com.
Escape character is '^]'.
220 VI1EUR06FT009.mail.protection.outlook.com Microsoft ESMTP MAIL Service ready at Sun, 13 Aug 2023 21:08:25 +0000
HELO U
250 VI1EUR06FT009.mail.protection.outlook.com Hello [142.132.196.110]
MAIL FROM: <tom@pentesttux.de>
250 2.1.0 Sender OK
RCPT TO: <livehacking@outlook.de>
250 2.1.5 Recipient OK
DATA
354 Start mail input; end with <CRLF>.<CRLF>
From: "Kent, Clark" <clark.kent@smallville.us>
To: "LiveHacking" <livehacking@outlook.de>
Subject: Best wishes from Smallville

Hello LiveHacking,

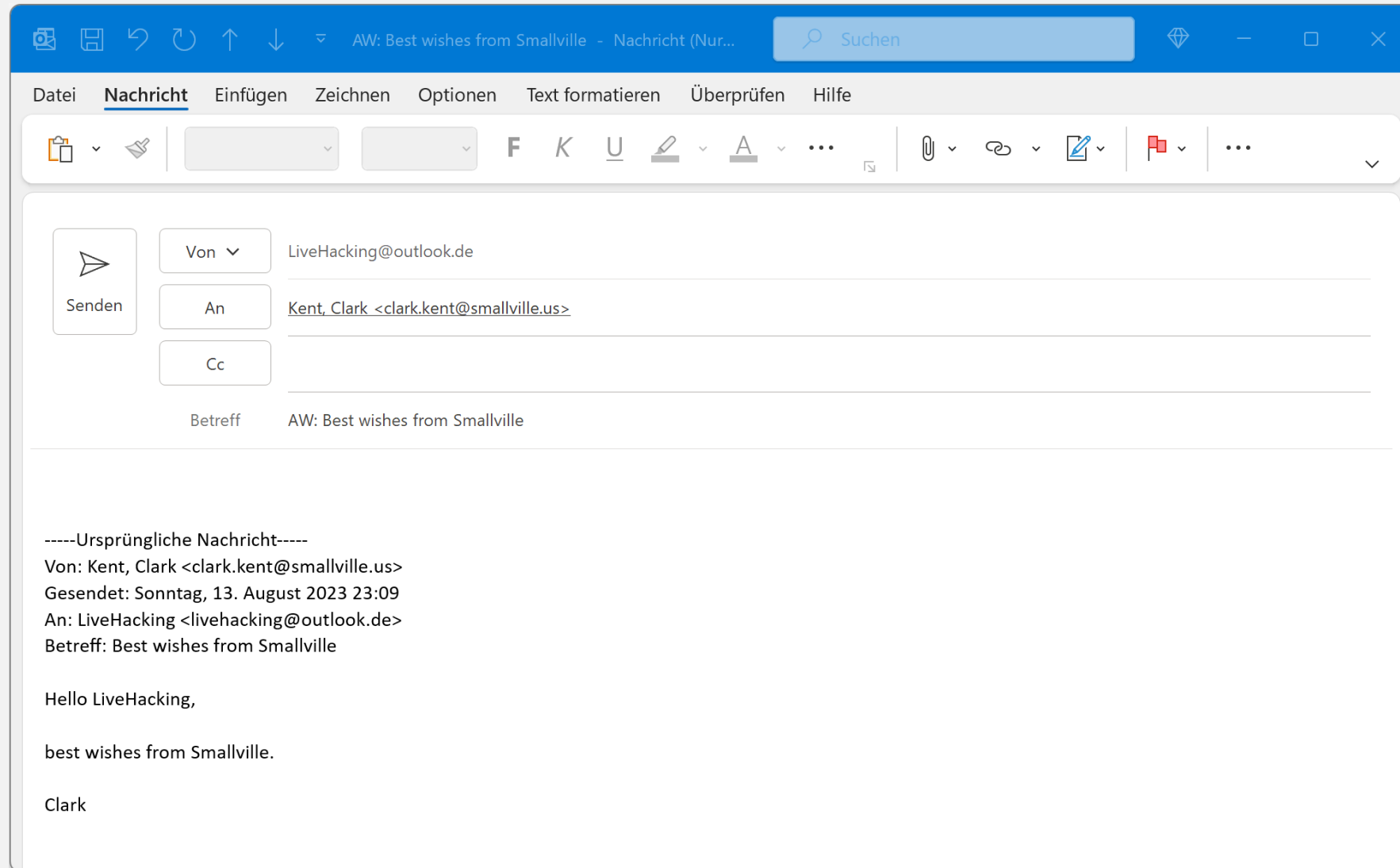
best wishes from Smallville.

Clark
.
250 2.6.0 <38c642aa-c653-4cf0-8edc-326de0183df7@VI1EUR06FT009.eop-eur06.prod.protection.outlook.com> [InternalId=77738
90807787, Hostname=DB9P195MB1633.EURP195.PROD.OUTLOOK.COM] 7724 bytes in 26.922, 0.280 KB/sec Queued mail for delivery
-> 250 2.1.5
```

Und so sieht es aus ...



Und die Antwort geht an ...



The screenshot shows an Outlook window with the title bar 'AW: Best wishes from Smallville - Nachricht (Nur...)'. The ribbon includes 'Datei', 'Nachricht', 'Einfügen', 'Zeichnen', 'Optionen', 'Text formatieren', 'Überprüfen', and 'Hilfe'. The 'Nachricht' ribbon is active, showing icons for attachments, a dropdown menu, and text formatting options (Bold, Italic, Underline, Text Color, Background Color). The email header shows a 'Senden' button with a paper plane icon. The 'Von' field is 'LiveHacking@outlook.de'. The 'An' field is 'Kent, Clark <clark.kent@smallville.us>'. The 'Cc' field is empty. The 'Betreff' field is 'AW: Best wishes from Smallville'. The email body contains the following text:

-----Ursprüngliche Nachricht-----
Von: Kent, Clark <clark.kent@smallville.us>
Gesendet: Sonntag, 13. August 2023 23:09
An: LiveHacking <livehacking@outlook.de>
Betreff: Best wishes from Smallville

Hello LiveHacking,

best wishes from Smallville.

Clark

Und wie ist es bei der Telekom?

```
tomo — tomo@TOMO-MBP — — -zsh — 90x28
[tomo@TOMO-MBP] — [~] — [2023-08-13 10:29:19]
[0] <> dig telekom.de MX

; <<>> DiG 9.10.6 <<>> telekom.de MX
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 64133
;; flags: qr rd ra; QUERY: 1, ANSWER: 5, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
;; QUESTION SECTION:
;telekom.de.                IN      MX

;; ANSWER SECTION:
telekom.de.                3600    IN      MX      100 mailin32.telekom.de.
telekom.de.                3600    IN      MX      100 mailout32.telekom.de.
telekom.de.                3600    IN      MX      100 mailin42.telekom.de.
telekom.de.                3600    IN      MX      100 mailin12.telekom.de.
telekom.de.                3600    IN      MX      100 mailin22.telekom.de.

;; Query time: 48 msec
;; SERVER: 192.168.10.1#53(192.168.10.1)
;; WHEN: Sun Aug 13 22:29:40 CEST 2023
;; MSG SIZE rcvd: 165

[tomo@TOMO-MBP] — [~] — [2023-08-13 10:29:52]
[0] <>
```

Keine Mails aus dem Homeoffice

Der Versand einer Email vom Homeoffice funktioniert nicht unbedingt. Der Telekom Mailserver erkennt, dass es sich um eine dynamisch zugewiesene IP-Adresse eines ISP handelt und verweigert daher den Verbindungsaufbau.

```
tomo — tomo@TOMO-MBP — ~ — zsh — 96x28
[tomo@TOMO-MBP] - [~] - [2023-08-13 10:30:24]
[0] <> telnet mailin32.telekom.de smtp
Trying 194.25.225.196...
Connected to mailin32.telekom.de.
Escape character is '^]'.
554-MAILIN32.telekom.de
554 Your access to this mail system has been rejected due to the sending MTA's poor reputation.
If you believe that this failure is in error, please contact the intended recipient via alternative means.
Connection closed by foreign host.
[tomo@TOMO-MBP] - [~] - [2023-08-13 10:31:08]
[1] <> █
```

Das war ...

Das ist aber spoofy ...

Tom Gries (TOMO) | September 2023



@tomo@chaos.social



2023-09-02