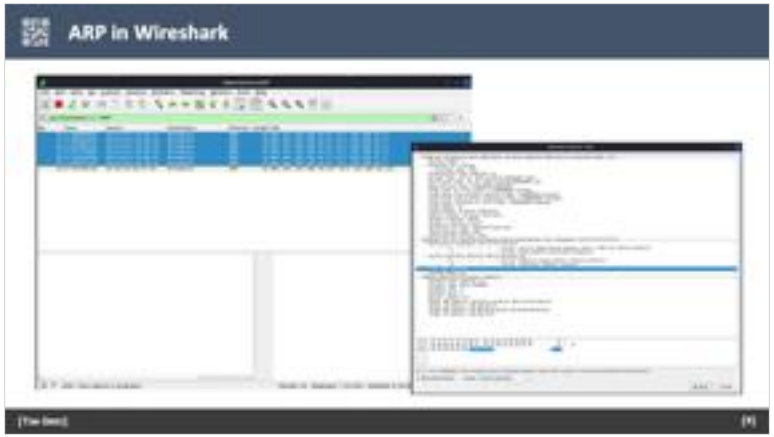
# Allgemeine Sicherheitsaspekte in der Adressierung

Tom Gries

Dokumenten URL: http://docs.tx7.de/TT-SA5
Autor: Tom Gries <TT-SA5@tx7.de>
@tomo@chaos.social


Version: 7.3.0 vom 22.07.2025

# ARP-Spoofing




| ARP Table (arp –a) | |
|---|---|
| IP-Adresse | MAC-Adresse |
| 192.168.44.8 | FE:12:BB:A1:B4:88 |

| ARP Table (arp –a) | |
|---|---|
| IP-Adresse | MAC-Adresse |
| 192.168.44.7 | FE:12:BB:A1:B4:77 |

A

192.168.44.7
FE:12:BB:A1:B4:77

B

192.168.44.8
FE:12:BB:A1:B4:88

Angreifer:

192.168.44.9
FE:12:BB:A1:B4:99

X

| ARP Table (arp –a) - gespooft | |
|---|---|
| IP-Adresse | MAC-Adresse |
| 192.168.44.8 | FE:12:BB:A1:B4:99 |

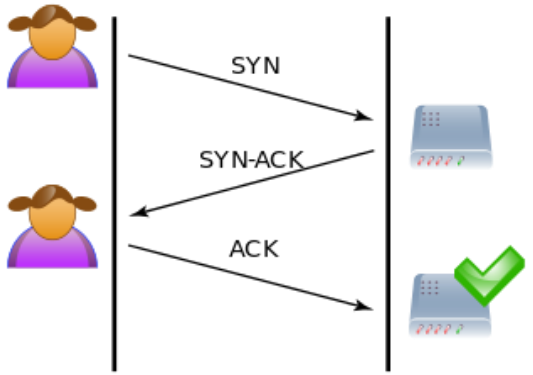
| ARP Table (arp –a) - gespooft | |
|---|---|
| IP-Adresse | MAC-Adresse |
| 192.168.44.7 | FE:12:BB:A1:B4:99 |

# DoS und DDoS

Im Unterschied zu anderen Angriffen will der Angreifer beim DoS-Angriff nicht in den Computer eindringen, sondern das System überlasten. Wird diese Art von Angriff von einer Vielzahl von Rechnern durchgeführt, spricht man von einem DDoS (**Distributed Denial of Service**). Daher werden keine Passwörter oder Ähnliches vom Zielrechner benötigt.

Eine (D)DoS Attacke wird auch durchgeführt, um die Verteidiger zu binden und um vom eigentlichen Angriff abzulenken. Beispiele für einen DoS-Angriff sind unter anderem:

- ⇒ SYN-Flooding (SYN, SYN-ACK mit fehlendem ACK)
- ⇒ Ping of Death (ICMP Paket größer als MTU)
- ⇒ Smurfs Angriff (Ping an Broadcast mit IP des Opfers)



# DNS Spoofing mit HOSTS Datei

Beispiel einer lokalen HOSTS-Datei:

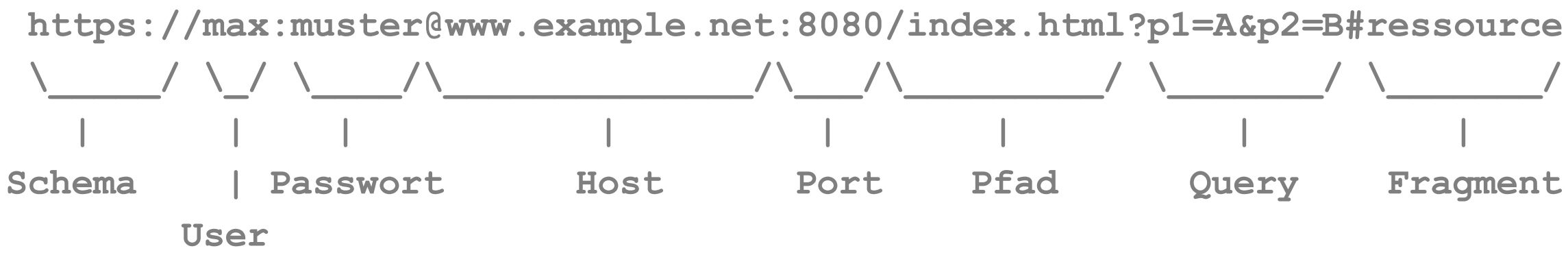
```
# This is a sample HOSTS file.
#
# This file is stored at C:\Windows\System32\drivers\etc\hosts
# on Windows machines and at /etc/hosts on Linux/Unix machines.


### Example for IP-Spoofing
40.114.177.156      example.net   ### IP of duckduckgo.com
0.0.0.0             facebook.com www.facebook.com
```

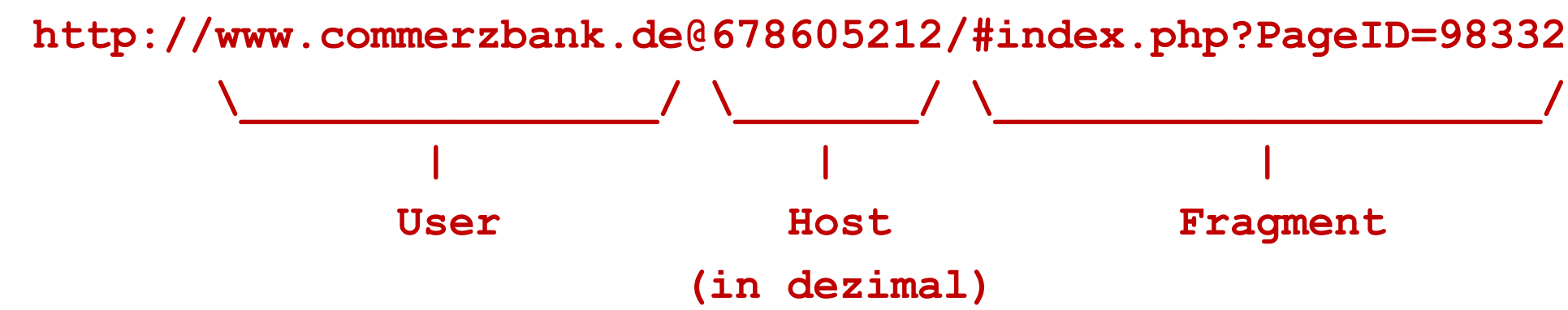
# URL Verschleierung

http://www.commerzbank.de@678605212/#index.php?PageID=98332

Scan me

# URL Verschleierung - Erklärung




Tipp 1: ping 678605212

Tipp 2: curl ifconfig.co

Tipp 3: http://ifconfig.co

# QR-Code Fake


**Frage:**

Welche Security-Aspekte sind bei QR-Codes zu beachten?

# Anmerkungen oder Fragen?

# ARP in Wireshark