# Sicherheitsaspekte in der Adressierung

## Spoofing und Verschleierung

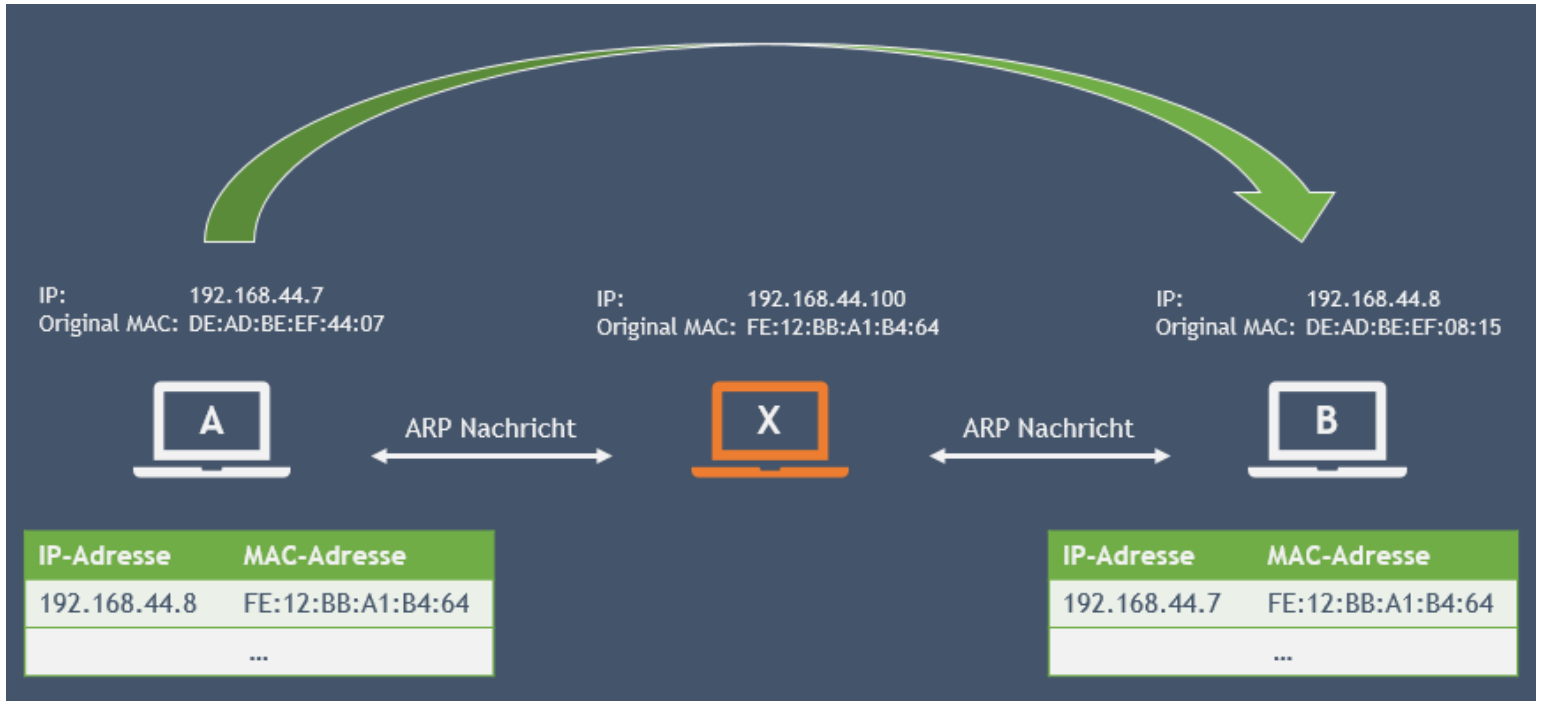
Tom Gries | Berlin | Oktober 2023

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


Version: 7.0.0 vom 20.10.2023

# ARP-Spoofing

ARP-Spoofing ist eine "Man-in-the-Middle" Attacke. Der Angreifer sitzt dabei im lokalen Netz. Dadurch wird der Datenverkehr zum Angreifer umgeleitet. In der Folge können dann Datenpakete mitgelesen, gefälscht oder gedroppt werden. Anm.: ARP bzw. MAC-Adressen kennen kein Routing.

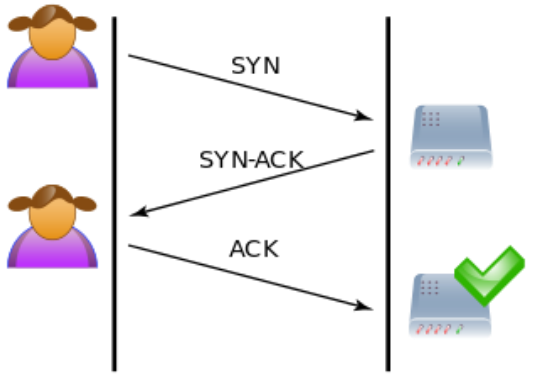


# DoS und DDoS

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:

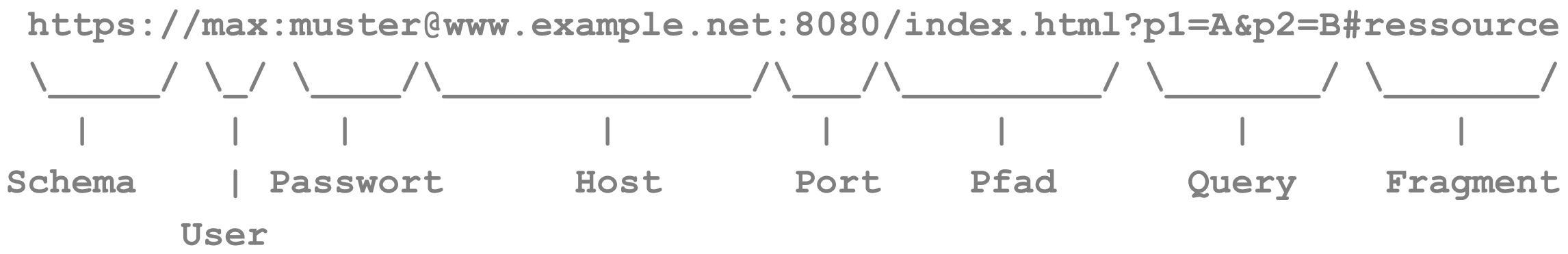
```
# This is a sample HOSTS file.
#
# This file is stored at C:\Windows\System32\drivers\etc\hosts
# on Windows machines and at /etc/hosts on Linux/Unix machines.


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

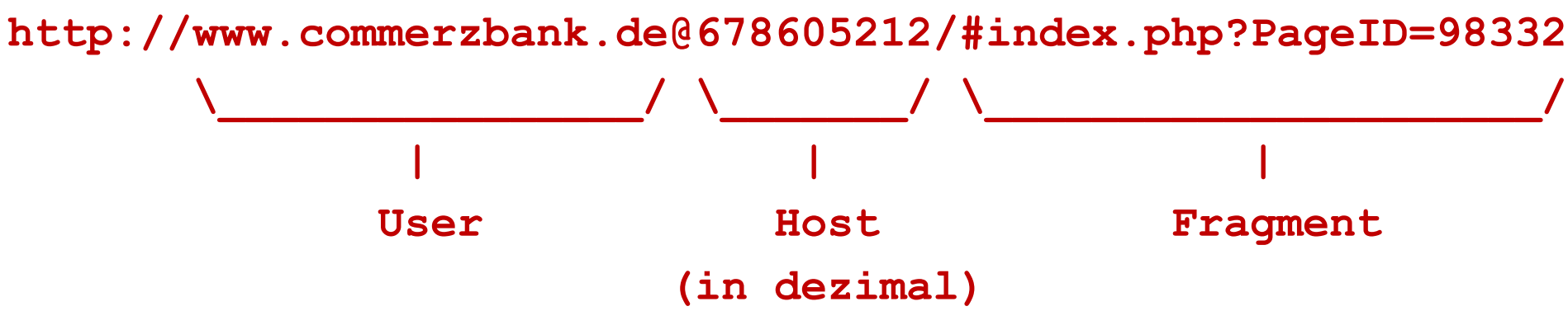
# URL Verschleierung

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

Scan me

# URL Verschleierung - Erklärung




Tipp: ping 678605212

# QR-Code Fake


**Frage:**

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

# Anmerkungen oder Fragen?