

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

Lizenz:

Creative Commons BY-NC-ND

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



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

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

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



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

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

Angreifer:

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



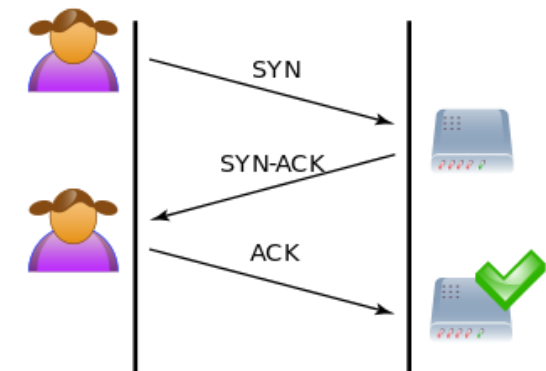


DoS und DDoS

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



`https://max:muster@www.example.net:8080/index.html?p1=A&p2=B#ressource`

_____/\	_/\	_____\	/_____/\	/_____/\	/_____/\	/_____/\	/_____/\
Schema	User	Password	Host	Port	Pfad	Query	Fragment

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

_____/\ _____/ _____/\

| | |

User Host Fragment

(in dezimal)

Tipp 1: ping 678605212

Tipp 2: curl ifconfig.co

Tipp 3: <http://ifconfig.co>



QR-Code Fake



ERLEBEN, WAS VERBINDET.

DER ALPTRAUM FÜR HACKER
PENETRATIONSTEST KOMPAKT



KONTAKT

- Persönlicher Kundenberater
- freecall 0800 33 01300
- Für alle Produktdetails folgen Sie dem QR-Code:



HERAUSGEBER

Telekom Deutschland GmbH
Landgrabenweg 151
53227 Bonn

Stand 04/2019 | Änderungen und Irrtümer

Frage:

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

Anmerkungen oder Fragen?



ARP in Wireshark

The image displays the Wireshark network protocol analyzer interface. The main window shows a packet capture from the `eth0` interface, filtered by `_ws.col.protocol == "ARP"`. The packet list shows several ARP requests (Who has 192.168.44.8? Tell 192.168.44.77) and one ARP request (Who has 192.168.10.21? Tell 192.168.10.127). The packet details pane on the right shows the structure of the selected ARP request (Frame 13).

Packet List:

No.	Time	Source	Destination	Protocol	Length	Info
13	2.868866626	Parallels_e3:0e:2a	Broadcast	ARP	42	Who has 192.168.44.8? Tell 192.168.44.77
14	3.898260252	Parallels_e3:0e:2a	Broadcast	ARP	42	Who has 192.168.44.8? Tell 192.168.44.77
16	4.921960710	Parallels_e3:0e:2a	Broadcast	ARP	42	Who has 192.168.44.8? Tell 192.168.44.77
17	5.947754503	Parallels_e3:0e:2a	Broadcast	ARP	42	Who has 192.168.44.8? Tell 192.168.44.77
18	6.972189420	Parallels_e3:0e:2a	Broadcast	ARP	42	Who has 192.168.44.8? Tell 192.168.44.77
19	7.994271170	Parallels_e3:0e:2a	Broadcast	ARP	42	Who has 192.168.44.8? Tell 192.168.44.77
20	8.307355129	ba:48:c4:3a:f7:92	Broadcast	ARP	42	Who has 192.168.10.21? Tell 192.168.10.127

Packet Details (Frame 13):

- Section number: 1
- Interface id: 0 (eth0)
- Interface name: eth0
- Encapsulation type: Ethernet (1)
- Arrival Time: Jul 27, 2025 17:16:20.930510057 CEST
- UTC Arrival Time: Jul 27, 2025 15:16:20.930510057 UTC
- Epoch Arrival Time: 1753629300.930510057
- Time shift for this packet: 0.000000000 seconds
- Time delta from previous captured frame: 1.098858750 seconds
- Time delta from previous displayed frame: 0.000000000 seconds
- Time since reference or first frame: 2.868866626 seconds
- Frame Number: 13
- Frame Length: 42 bytes (336 bits)
- Capture Length: 42 bytes (336 bits)
- [Frame is marked: False]
- [Frame is ignored: False]
- [Protocols in frame: eth:ethertype:arp]
- [Coloring Rule Name: ARP]
- [Coloring Rule String: arp]
- Ethernet II, Src: Parallels_e3:0e:2a (00:1c:42:e3:0e:2a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
- Destination: Broadcast (ff:ff:ff:ff:ff:ff)
- Source: Parallels_e3:0e:2a (00:1c:42:e3:0e:2a)
- Type: ARP (0x0806)
- [Stream index: 8]
- Address Resolution Protocol (request)
- Hardware type: Ethernet (1)
- Protocol type: IPv4 (0x0800)
- Hardware size: 6
- Protocol size: 4
- Opcode: request (1)
- Sender MAC address: Parallels_e3:0e:2a (00:1c:42:e3:0e:2a)
- Sender IP address: 192.168.44.77
- Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
- Target IP address: 192.168.44.8

Packet Bytes:

```
0000 ff ff ff ff ff 00 1c 42 e3 0e 2a 08 06 00 01 ..... B-.*....
0010 08 00 06 04 00 01 00 1c 42 e3 0e 2a c0 a8 2c 4d ..... B-.*.,M
0020 00 00 00 00 00 00 c0 a8 2c 08 ..... .C..
```

Status Bar: eth0: <live capture in progress> Packets: 32 · Displayed: 7 (21.9%) · Selected: 6 (18.8%)