

Wesentliche Protokolle

HTTP(S), FTP(S), DHCP, SMTP, POP4, IMAP4 und Spoofing mit Telnet

Tom Gries



Dokumenten URL:

<http://docs.tx7.de/TT-PRT>

Autor:

Tom Gries <TT-PRT@tx7.de>
@tomo@chaos.social

Lizenz:

Creative Commons BY-NC-ND

Version:

7.2.0 vom 02.02.2024





HTTP(S)

Jeder Webserver "spricht" **HTTP**. In den letzten Jahren auch immer mehr die verschlüsselte Variante **HTTPS**.

HTTP ist ein Klartextprotokoll. Wenn man den Aufbau kennt, kann man mit Telnet "httpisch sprechen".

```
Kali - LiveHacking
root@TOMO-DesktopPC:~# telnet example.net http
Trying 93.184.216.34...
Connected to example.net.
Escape character is '^]'.
GET / HTTP/1.0
HOST: example.net
```



FTP(S)/(S)FTP

FTP ist eins der ältesten Protokolle und Anwendungen. In den Anfangszeiten des Internets wurden so Daten ausgetauscht (HTTP gab es da noch nicht).

FTP wird in aktiv und passiv unterschieden.

```
Kali - LiveHacking
root@TOMO-DesktopPC:~# ncftp ftp.uni-kl.de
NcFTP 3.2.5 (Feb 02, 2011) by Mike Gleason (http://www.NcFTP.com/contact/).
Connecting to 131.246.123.4...
(vsFTPD 2.3.2)
Logging in...
*****
***      Welcome to the Anonymous FTP Server at the      ***
***                        University of Kaiserslautern      ***
*****

If you have any problems, ideas or whatever, please feel
free to write an Electronic Mail to

ftpadm@uni-kl.de

*****
ALL TRANSFERS WILL BE LOGGED
*****
Login successful.
Logged in to ftp.uni-kl.de.
ncftp / > bye
```



DHCP steht für „Dynamic Host Configuration Protocol“. Es ermöglicht die Zuweisung der Netzwerkkonfiguration, wie zum Beispiel

- IP Adresse (IPv4 und/oder IPv6)

- Subnetmask

- Default Gateway

- Nameserver (DNS – Primary und/oder Secondary)

- NTP-Server

- Hostname

an Clients durch einen Server für eine bestimmte Zeit (Lease Time).

Anmerkungen oder Fragen?