

Aufgabe 1 (IP-Adressen finden)

Welche IP-Adressen haben die folgenden Rechner:

Anfragenname	IP-Adresse	Echter Name zur Adresse
www.uni-kl.de	131.246.120.51	www.uni-kl.de
www.ebay.com	66.135.214.176 66.135.194.100	hp-core.ebay.com
www.cs.waikato.ac.nz	130.217.247.31	gollum.cs.waikato.ac.nz
www.stanford.edu	171.67.22.26	www1.Stanford.EDU
www.microsoft.com	207.46.192.254 207.46.193.254 207.46.19.190 207.46.19.254	wwwtk2test1.microsoft.com wwwtk2test2.microsoft.com wwwbaytest1.microsoft.com wwwbaytest2.microsoft.com
java.sun.com	72.5.124.55	nicht auffindbar
www.redbooks.ibm.com	207.25.253.45	dispsd-45- redbk.boulder.ibm.com

Der Befehl dafür heißt nslookup

Aufgabe 2 (Server finden)

a) Um eine email an eine Adresse der xyz@wolke7.net zu senden, muß die Adresse des Mail-Servers von wolke7.net bekannt sein. Wie lautet die Adresse des Mail-Servers von wolke7.net?

Das kann man mit `dig wolke7.net mx` herausfinden.

Die Antwort ist: `mx0.gmx.net`

b) Die Deutsche Bank AG hat einen eigenen Internetauftritt und verschiedene Rechner im Internet. Wie heißt der für die Domäne deutsche-bank.de zuständige Nameserver und welche IP-Adresse hat er?

`dig deutsche-bank.net ns:`

`ns1.deutsche-bank.de` und `ns2.deutsche-bank.de`

Aufgabe 3 (Nicht-Rekursive Anfrage stellen)

Überlegen sie sich eine exotische DNS Domain und stellen eine nicht rekursive Anfrage an den DNS-Server zu diesem Domain-Namen. Interpretieren sie die Antwort des DNS-Servers.

Die Antwort des DNS-Servers enthält jene Nameserver, die die Adresse am weitesten (von hinten) auflösen können.

Aufgabe 4 (Caching Parameter)

In der ersten Zeile der zoneDateien stehen Informationen über die Art und Weise, wie Informationen im Cache verwaltet werden und wie Primary Master und Secondary Master sich beim zone transfer verhalten. Die Details sind in RFC 1035 spezifiziert. Welche Bedeutung haben die folgenden Parameter?

a) Refresh

A 32 bit time interval before the zone should be refreshed

b) Retry

A 32 bit time interval that should elapse before a failed refresh should be retried

c) Expire

A 32 bit time value that specifies the upper limit on the time interval that can elapse before the zone is no longer authoritative

d) Minimum

The unsigned 32 bit minimum TTL field that should be exported with any RR from this zone

Aufgabe 5 (Sicherheitsfragen)

a) Wieso ist es eigentlich ein Problem, wenn ein Hacker es schafft, seine eigene IP-Adresse mit einem fremden DNS-Namen zu verknüpfen, so dass ein Surfer im Internet nicht auf den richtigen Seiten landet? Beschreiben Sie hierbei was passiert, welche Risiken dadurch entstehen und welcher Schaden dadurch angerichtet werden kann.

Anfragen an den DNS-Namen werden zum Hacker-PC umgeleitet. Dieser kann präparierte Online-Inhalte zur Verfügung stellen, um Opfer zu täuschen und ihnen beispielsweise vertrauliche Daten zu entlocken.

Weiterhin wird die IP-Adresse des Hacker-PCs im Cache des PC gespeichert. Wenn also die falsche Umleitung von einer anderen Instanz im Netzwerk entdeckt wird, kann sie nicht verhindern, daß die im Cache befindliche IP-Adresse des Hacker-PCs weiterhin zum Routen verwendet wird.

b) Warum muß ein Hacker gar keinen DNS-Server manipulieren, um auf einem Microsoft Windows PC dafür zu sorgen, dass ein offizieller DNS-Name (z.B. der einer Bank) auf die IP-Adresse des Hackers abgebildet wird?

Die Hosts-Datei unter %system%/system32/drivers/etc/ kann auch von nicht-privilegierten Benutzern geändert werden. Der Hacker könnte also beispielsweise ein ActiveX-Skript ins Netz stellen, das die Hosts-Datei verändert. Unter Linux kann die Datei nur von Benutzern mit Root-Rechten verändert werden.