# Übung zur Netzwerkkonfiguration und –analyse

## a.) Lokale Konfiguration

1. Öffnen Sie ein DOS-Fenster und lassen Sie sich mit dem Programm **ipconfig.exe** zur IP-Konfigurationskontrolle die TCP/IP-Daten Ihres Rechners anzeigen. Informieren Sie sich über die Optionen von ipconfig ? und lassen Sie sich die NetzkartenID (MacID) anzeigen.
2. Testen Sie mit dem Programm **ping.exe** die Erreichbarkeit des Gateway-Rechners aus 1 und Ihres Nachbarrechners
3. Wie kann mit ping ein Dauertest eines Rechners, z.B. zur Ausfallkontrolle, erfolgen ? Was bedeutet der Parameter TTL bei ping ?

4. Lassen Sie sich die IP-Aktivitäten Ihres Rechners mit netstat anzeigen. Testen Sie mit dem Befehl netstat –a –n 1 den Anruf von verschiedenen Internetseiten. Testen Sie die weiteren Optionen von netstat. Welche Informationen sind besonders sicherheitsrelevant ?

5. Führen Sie einen Portscan Ihres Rechners über http://www.dnstools.ch/port-scanner.html bzw. bei Nicht-Proxy-Zugriff auch über http://www.heise.de/security/dienste/portscan/test/go.shtml?scanart=1 durch. Welche Ursachen können Differenzen zu den netscan-Ergebnissen haben ?

6. Wie kann ein Klasse-C-Netz in 4 Subnetze zerlegt werden ? Welche IP-Host-Adressen können dabei jeweils vergeben werden ?

## b.) Analyse entfernter Netze und Rechner

7. Ermitteln Sie mit dem Programm tracert (bzw. für die ausländischen Adressen mit http://www.heise.de/netze/tools/traceroute) die IP-Adressen und Routen zu folgenden Servern. Welche gleichen Teilwege existieren ?

| | |
|---|---|
| 141.56.132.164 | Wie heißt der Rechner selbst ? |
| www.tu-dresden.de | |
| mit.edu | |
| www.microsoft.de | Beachten Sie die Zeiten ! |
| ftp.denic.de | |

8. Wie arbeitet tracert ? (vgl. Heise-Netzwerk-Website)
9. Zur noch besseren Visualisierung können Sie auch über http://www.dnstools.ch/visual-traceroute.html eine grafische Darstellung generieren.

10. Wem gehört die Domäne dtag.de und wann wurde diese angemeldet ? Beantworten Sie diese Frage mittels www.denic.de ! Welche Domänen werden von DENIC verwaltet ? Wie ist in etwa das Verhältnis der .de-Domanins zu den anderen großen Domains ? Was ist ein Dispute-Eintrag ?
11. Informieren Sie sich bei DENIC über die Anzahl der z.Z. registrierten Domänen. In welcher Stadt sind die meisten deutschen Domäns pro Einwohner registriert ?

12. Welche RFC-Richtlinien befassen sich mit den neuen „Internationalized Domain Names“ (IDN) ? Was ist ein Punycode ?

13. In einem Serverlog taucht die IP-Adresse 164.67.128.33 mehrfach mit verdächtigen Aktionen auf. Von wo erfolgen wahrscheinlich die Zugriffe (Einrichtung und Ort) und wen müssten Sie anmailen, um den Verantwortlichen zu informieren ?

14. Wie können weiterführende Informationen über die potentiellen Angriffe aus 13. möglichst effektiv gesammelt werden ?

15. Wie lauten der Namen der Mailserver der Universität Rostock ? Sind diese per Ping erreichbar ?

## c.) Weiterführende Literatur und Quellen

16. Informieren Sie sich unter http://www.heise.de/security/ über aktuelle Sicherheitsprobleme.

17. Welche Toolsuite wird vom Bundesamt für Sicherheit in der Informationstechnik (www.bsi.bund.de) bereit gestellt. Informieren Sie sich weiterhin über die Bandbreite der beim Amt laufenden Arbeiten und verfügbaren Themen.