Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Dr. Helmut Reiser

MNM TEAM
Munich Network Management Team

# IT-Sicherheit im Wintersemester 2008/2009
# Übungsblatt 1

**Abgabetermin:** 29.10.2008 bis 14:00 Uhr

**Achtung:** Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikums Infrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungs Webseite zum Übungsberieb an.

Die schriftlichen Lösungen aller mit H gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben. Während des Semesters werden drei Übungsblätter korrigiert. Bei drei richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei zwei richtigen Lösungen erhalten Sie einen Notenbonus von einer drittel Notenstufe.

## Aufgabe 1: (H) SQL-Slammer

a. Skizzieren Sie anhand der in der Vorlesung genannten Eckwerten die statistische Ausbreitung von SQL-Slammer innerhalb der ersten Minute. Wie viele Instanzen von SQL-Slammer existieren nach 60 Sekunden?

b. Wie ist die maximal beobachtete Probing Rate von 26.000 Hz begründbar?

c. Warum verlangsamt sich das Wachstum der Ausbreitungsgeschwindigkeit nach ca. 60 Sekunden?

d. Wie viele Infektionsversuche pro Sekunde werden nach 60 Sekunden von allen infizierten Systemen in Summe durchgeführt?

e. Wie lange dauert es, bis 80% der an das Internet angebundenen, verwundbaren Systeme infiziert sind? Gehen Sie davon aus, dass sich die Population der infizierten Systeme im Schnitt alle ca. 37 Sekunden verdoppelt.

## Aufgabe 2: (K) OSI Security Architecture

a. Erläutern Sie die Begriffe Integrity, Confidentiality, Non-repudiation, Authentication!

b. Im Skript wird eine Zuordnung von sicherheitsrelevanten Services auf OSI Schichten gegeben, die in folgender Tabelle noch einmal dargestellt wird.

| | OSI-Layer | | | | | | |
|---|---|---|---|---|---|---|---|
| Service | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| peer entity authentication | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ |
| data origin authentication | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ |
| access control service | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ |
| connection confidentiality | ✔ | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ |
| connectionless confidentiality | ✘ | ✔ | ✔ | ✔ | ✘ | ✔ | ✔ |
| selective field confidentiality | ✘ | ✘ | ✘ | ✘ | ✘ | ✔ | ✔ |
| traffic flow confidentiality | ✔ | ✘ | ✔ | ✘ | ✘ | ✘ | ✔ |
| connection integrity with recover | ✘ | ✘ | ✘ | ✔ | ✘ | ✘ | ✔ |
| connection integrity without recover | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ |
| selective field connection integrity | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✔ |
| connectionless integrity | ✘ | ✘ | ✔ | ✔ | ✘ | ✘ | ✔ |
| selective field connectionless integrity | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✔ |
| non-repudiation origin | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✔ |
| non-repudiation deliver | ✘ | ✘ | ✘ | ✘ | ✘ | ✘ | ✔ |

Ordnen Sie die nachfolgenden Begriffe in diese Tabelle ein. Was stellen Sie fest?

- Dedizierte Leitung
- WEP
- HMAC-SHA
- IPSEC AH
- DES
- Hot Potato
- SSL-VPN
- WPA2
- PGP
- SSL
- 3DES
- WPA
- IPSEC ESP
- TLS
- RSA
- Flooding
- DSA
- VLAN
- HMAC-MD5
- EAP
- X.509
- CRC
- MD5
- CDMA
- AES
- SHA