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 2009/2010
Übungsblatt 1

Abgabetermin: 04.11.2009 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 (per Email, in der Vorlesung oder vor der Übung). Während des Semesters werden vier Übungsblätter korrigiert. Bei vier richtigen Lösungen erfolgt ein Bonus von zwei drittel Notenstufen auf die Klausurnote, bei nur drei oder 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?

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.

Service	OSI-Layer 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	✘	✘	✘	✘	✘	✘	✔

Erläutern Sie die folgenden Begriffen kurz? Versuchen Sie die Begriffe in die Tabelle einzuordnen.

- IPSEC AH
- IPSEC ESP
- AES
- WPA2
- CRC
- SHA
- SSL
- MD5
- 3DES
- CDMA
- RSA

Aufgabe 3: (T) W32.Conficker / W32.Downadup

a. Skizzieren Sie in Einzelschritten die Infektion eines Microsoft Windows Rechners mit dem Conficker-Wurm Variante A? Welche Schwachstellen erkennen Sie?

b. Wie funktioniert der Algorithmus für die Domaingenerierung? Was versteht man im Umfeld von Conficker unter dem Rendezvous-Protokoll?

c. Beschreiben Sie die Schritte des Binary Downloads. Welche Sicherheitsmechanismen werden eingesetzt? Was könnte der Grund für diesen Aufwand sein?

d. Welche Propagations-Mechanismen besitzt Conficker allgemein. Berücksichtigen Sie bei Ihrer Antwort auch weitere Varianten des Wurms.

e. Welche Detektionsmöglichkeiten haben Sie in großen Netzen wie z.B. dem MWN? Welche Gegenmaßnahmen könnten Sicherheitsexperten eingeleitet haben?