Ludwig-Maximilians-Universität München
Institut für Informatik
Lehr- und Forschungseinheit für Kommunikationssysteme und Systemprogrammierung
Prof. Dr. Helmut Reiser, PD Dr. Wolfgang Hommel

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2015/2016
Übungsblatt 7

Abgabetermin: 15.12.2015 bis 12:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben ist es notwendig sich über den Vorlesungsinhalt hinaus, durch Internet- und Literaturrecherche mit dem Thema zu beschäftigen.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (über Uniworx als **Einzelabgabe**). Während des Semesters werden vier Übungsblätter ausgewählt, korrigiert und bewertet. Bei vier als korrekt bewerteten Lösungen (mind. 75% der erreichbaren Punkte) 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.

Bei Fragen zu Übungsaufgaben sowie generellen Anregungen, Verbesserungsvorschlägen, ... zum Übungsbetrieb wenden Sie sich bitte per Email an **`uebung-itsec@lrz.de`**.

Aufgabe 20: (H) Social Engineering (13 Punkte)

In der Vorlesung wurde ausführlich das Thema *Social Engineering* vorgestellt.

a. Nennen und erläutern Sie Kriterien bzw. leiten Sie daraus Kategorien ab, in die sich Social Engineering Angriffe sinnvoll einteilen lassen.

b. Eine Möglichkeit, dass ein Social Engineer an sensible Informationen gelangt, ist *Phishing*. Erläutern Sie die Phishing-Varianten *Clone phishing*, *Spear phishing* und *Whaling*.

c. Nennen Sie mindestens 4 Dinge, die eine Phishing-E-Mail aufweisen sollte, damit der Social Engineer sein Ziel, d.h. das Erlangen sensibler Informationen, z.B. Zugangsdaten, erreicht.

d. Erstellen Sie eine fiktive Phishing-E-Mail, die Ihren Übungsleiter dazu verleitet, Ihnen die Zugangsdaten für Uniworx mitzuteilen, womit Sie in der Lage wären, sowohl Musterlösungen für Hausaufgaben als auch Klausuren einzusehen.

e. Als wirkungsvollste Maßnahme gegen Social Engineering Angriffen gilt nach wie vor, Mitarbeiter zu sensiblisieren und der Aufbau eines Security Awareness Programms. In der vom SANS-Institut herausgegebenen *Top 20 Security Controls* Liste wird auch das Control *Security Skills Assessment and Appropriate Training to Fill Gaps* angeführt. Nennen und erläutern Sie die insgesamt fünf wichtigen Aspekte, diese Maßnahme erfolgreich umzusetzen.

Aufgabe 21: (H) Grundlagen Kryptographische Systeme & DES (10 Punkte)

a. Wie definiert man allgemein ein kryptographisches System bzw. Kryptosystem? Welche Unterschiede bestehen hierbei zwischen einem symmetrischen und einem asymmetrischen Verfahren?

b. Erklären Sie die Begriffe bzw. Verfahren *Substitution* und *Permutation*? Welche der beiden Verahren setzt z.B. der bekannte symmetrische Verschlüsselungsalgorithmus DES ein? Falls Permutationen verwendet werden, würden Sie sagen, dass sich dadurch die Stärke des DES-Verfahrens erhöht?

c. Kryptoanalytiker oder auch Angreifer versuchen beispielsweise an verschlüsselt übertragene Informationen oder den bei der Verschlüsselung verwendeten Schlüssel zu gelangen? Dazu existieren verschiedene Vorgehensweisen. Erläutern Sie den Ablauf eines *Chosen-Plaintext*- bzw. *Chosen-Ciphertext-Angriffs*.

d. Was versteht man allgemein unter sogenannten *Seitenkanalangriffen*?

e. In der Vorlesung wurde der Ablauf der Algorithmen DES als auch 3DES erläutert, wobei bei 3DES grundsätzliche eine Hintereinanderausführung von Verschlüsselungs- und Entschlüsselungsschritten erfolgt. Für die dabei verwendeten Schlüssel gibt es mehrere Möglichkeiten, die auch als *Keying options* bezeichnet werden. Nennen und erläutern Sie diese kurz.

f. Nennen und erläutern Sie noch je zwei Vor- bzw. Nachteile, die das DES-Verschlüsselungsverfahren aufweist.