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 2010/2011
Übungsblatt 2

Abgabetermin: 10.11.2010 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 4: (H) SYN Flooding Attacks

In der Vorlesung wurden verschiedende Angriffstechniken vorgestellt, u.a. auch SYN-Flooding Attacken.

a. Erläutern Sie in Stichpunkten den Ablauf von SYN-Flooding-Angriffen.

b. Als eine mögliche Gegenmaßnahme wurde der SYN-Cookie-Mechanismus vorgestellt. Beschreiben Sie die Funktionsweise von SYN-Cookies und nennen Sie Nachteile, die sich aus der Verwendung ergeben.

c. Neben SYN-Cookies existieren auch sog. RST-Cookies. Beschreiben Sie deren Funktionsweise.

d. Sie betreiben noch einen Microsoft Windows 2000 Server in Ihrem Rechenzentrum. Welchen Registry-Eintrag sollten Sie zur Vermeidung von SYN-Flooding-Attacken vornehmen?

Aufgabe 5: (K) Windows Password Hashverfahren

a. Windows verwendet unter anderem das LM Hashverfahren um Passwörter zu speichern, welches wie folgt arbeitet:

   (i) Das Passwort des Benutzers in Form eines OEM-String wird zu Großbuchstaben umgeformt.

   (ii) Dieses Passwort wird entweder auf 14 Bytes mit Nullen gefüllt oder gekürzt.

   (iii) Das Passwort mit der festen Länge wird in zwei 7 Byte-Hälften aufgeteilt.

(iv) Aus jeder Hälfte wird durch hinzufügen eines NON-Parity-BITs ein 64-BIT langer DES-Schlüssel erzeugt.

(v) Jeder dieser Schlüssel wird dazu genutzt, den Konstanten ASCII-String ”KGS!@#$%” zu DES-verschlüsseln, woraus zwei 8 Byte Chiffretext-Werte resultieren.

(vi) Diese beiden Chiffretext-Werte werden verbunden, um einen 16 Byte-Wert zu bilden, der den LM hash darstellt.

Bewerten Sie das eingesetzte Hashverfahren bezüglich seiner Sicherheit! Wie können die genannten Defizite entschärft werden?

Aufgabe 6: (K) Security Engineering

Security Engineering ist einer der zentralen Themen in der IT-Sicherheit. In der Vorlesung wurde Ihnen ein mögliches Vorgehensmodell erläutert. Versetzen Sie sich in die Lage eines Chief Information Security Officers eines mittelständischen Unternehmens mit ca. 500 angestellten Mitarbeitern. Sie haben von der Unternehmensleitung den Auftrag erhalten, die vorhandene IT-Infrastruktur (Mitarbeiter-PCs, Web-, File-, Datenbank-Server abzusichern. Wie gehen Sie vor?