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 2

Abgabetermin: 05.11.2008 bis 14:00 Uhr

Achtung: 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 3: (K) Syn-Cookies

Neuere Linux Versionen implementieren ein Verfahren, das als Syn-Cookies bekannt ist um Syn Flooding Angriffe zu unterbinden.

a. Erläutern Sie die Funktionsweise von Syn-Cookies und zeigen Sie, wie dadurch Syn-Flooding Attacken vermieden werden können!

b. Welche Nachteile haben Syn-Cookies?

c. Wie kann man Syn-Cookies unter Linux aktivieren?

Aufgabe 4: (H) Buffer-Overflow

Folgendes Programm ist gegeben:

```
#include <stdio.h>

int test() {

// initialisiere ein Array mit nur einem Eintrag
int i[1] = {42};

...

// Ausgabe des Array und Ende
printf("test: i[0] = %i\n\n", i[0]);
return i[0];
// -> Rücksprung ins aufrufende Programm
}
```

```
int main() {

// initialisiere x
// x sollte im Nachhinein den Wert 42 haben
int x = test();

printf("Dies ist ein Testprogramm.\n");
printf("Es demonstriert einen Puffer-Überlauf.\n\n");

// inkrementiere x
// x sollte im Nachhinein den Wert 43 haben
x++;

// Ausgabe von x und Ende
printf("main: x = %i\n", x);
return 0;
}
```

a. Ergänzen Sie das Programm an der gekennzeichneten Stelle so, dass die Inkrementierung von x in der `main()`-Routine nicht ausgeführt wird und am Ende x mit dem Wert 42 ausgegeben wird!

b. Erklären Sie das Phänomen!

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) 6. 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?