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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2011/2012
Übungsblatt 5

Abgabetermin: 30.11.2011 bis 14:00 Uhr

Achtung: Zur Bearbeitung einiger Übungsaufgaben benötigen Sie eine Rechnerkennung für unsere Praktikumsinfrastruktur. Um diese zu erhalten, melden Sie sich bitte über die Vorlesungswebseite zum Übungsbetrieb an.

Die schriftlichen Lösungen aller mit **H** gekennzeichneten Aufgaben sind **vor Beginn** der jeweils nächsten Übungsveranstaltung abzugeben (per **E-Mail** an die Adresse **uebung-itsec_AT_lrz.de** oder schriftlich 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 11: (H) Buffer-Overflow

Angreifer nutzen oftmals Schwachstellen in lokal installierten Applikationen.

a. Erläutern Sie knapp, was bei einem Buffer-Overflow genau passiert? Wie kann ein Angreifer dies ausnutzen?

b. Folgendes Programm ist gegeben:

```
1  #include <stdio.h>
2
3  char shellcode[] = "\xbb\x14\x00\x00\x00"
4                     "\xb8\x01\x00\x00\x00"
5                     "\xcd\x80";
6
7
8  int main() {
9
10     int *ret;
11
12     ret = (int *)&ret + <integer>;
13
14     (*ret) = (int)shellcode;
15 }
```

(i) Beschreiben Sie den grundsätzlichen Ablauf dieses Programms.

(ii) Der Stack habe bei Ausführung dieses Programms folgenden Aufbau (mithilfe von *gdb* und Breakpoint in Zeile 12 ermittelt):

0xbfa62f84:	0x08048350	0xbfa62fe8	0xb7df0390	0x00000001
0xbfa62f94:	0xbfa63014	0xbfa6301c	0xb7f262d0	0x00000000

Was verbirgt sich hinter den Werten *0x08048350* und *0xb7df0390*?

(iii) Ergänzen Sie den Programmtext an der Stelle *integer* (Zeile 12) mit dem korrekten Wert, damit der Shellcode in Zeile 14 (Adresse: 0x08049504) korrekt aufgerufen wird. Am Ende der Programmausführung sehe der Stack wie folgt aus:

0xbfa62f84:	0xbfa62f8c	0xbfa62fe8		0x00000001
0xbfa62f94:	0xbfa63014	0xbfa6301c	0xb7f262d0	0x00000000

Welcher Wert sollte in der Lücke nun stehen?

c. Betrachten Sie den gegebenen Shellcode. Welche Probleme könnten hierbei auftreten?

d. Welche Gegenmaßnahmen können Sie grundsätzlich ergreifen, um Buffer Overflow-Angriffen wirkungsvoll zu begegnen?

Aufgabe 12: (T) Buffer Overflow - Spawning a shell

In der vorherigen Aufgabe wurde das Thema "Buffer Overflow"behandelt. Eine mögliche Zielsetzung eines Hackers, der einen Buffer Overflow ausnutzt, ist das Starten einer Shell. In dieser Aufgabe soll ihnen gezeigt werden, wie man den ShellCode in beliebiger Umgebung ausführbar macht.