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 4

Abgabetermin: 17.11.2015 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 10: **(H)** SPAM-Protection (6 Punkte)

Der Versand von SPAM, welcher oftmals auf eine Infektion eines Systems mit einem Schadprogramm zurückzuführen ist, ist seit einigen Jahren ein großes Problem.

a. Es existieren verschiedene Maßnahmen, SPAM zu erkennen und diesen herauszufiltern bzw. zu blocken. Erläutern Sie folgende Verfahren: *DNS-basierte Blacklists*, *RHSBLs* und *naive Bayes-Klassifizierung*.

b. Welche rechtlichen Probleme könnten beim Einsatz bzw. dem Erstellen DNS-basierter Blacklists in Deutschland bestehen?

c. Eine weitere Methode, neben dem in der Vorlesung vorgestellten Greylisting, zur Bekämpfung von SPAM ist Sender-Policy-Framework (SPF). Beschreiben Sie kurz die Funktionsweise von SPF und geben sie einen exemplarischen SPF-Record an.

d. Vergleichen Sie kurz Greylists und SPF und nennen Sie Vor- und Nachteile. Berücksichtigen Sie dabei auch verschiedene Arten von E-Mail-Versand, wie z.B. E-Mail-Weiterleitungen etc.

e. SpamAssassin ist ein Programm, das mehrere Methoden zur Erkennung und Filterung von SPAM unterstützt. Beschreiben Sie kurz die Konfigurationsoptionen `use_bayes`, `use_learner`, `rewrite_header` und `required_score`.

Aufgabe 11: (H) Buffer-Overflow (8 Punkte)

Angreifer nutzen oftmals Schwachstellen in lokal installierten Applikationen.

a. Skizzieren und beschreiben Sie den Aufbau des Speichers eines Prozesses.

b. Erläutern Sie, was bei einem Buffer-Overflow genau passiert?

c. Erklären Sie, wie ein Angreifer einen Buffer-Overflow für einen Angriff ausnutzen könnte.

d. Beschreiben Sie den Unterschied zwischen einem klassischen Buffer-Overflow und einem return-to-libc Angriff.

e. Als wirksame Gegenmaßnahme gegen Buffer Overflows wurde die Address Space Layout Randomization (ASLR) eingeführt. Beschreiben Sie kurz die Funktionsweise von ASLR.

f. Welches Problem besteht bei ASLR insbesondere dann, wenn das Programm nicht als *Position Independent Executable (PIE)* kompiliert wurde?

g. Nennen und beschreiben Sie zwei weitere Schutzmaßnahmen (außer ASLR), die zum Schutz vor Buffer-Overflows eingesetzt werden können.

Aufgabe 12: (T) Shellcode

a. 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 }
```

b. Beschreiben Sie den grundsätzlichen Ablauf dieses Programms.

c. Welcher Wert muss anstelle von `<integer>` stehen, damit der Shellcode korrekt ausgeführt wird?

d. Wie kann überpüft werden, welche Funktion der Shellcode hat?