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

MNM TEAM
Munich Network Management Team

IT-Sicherheit im Wintersemester 2012/2013
Übungsblatt 3

Abgabetermin: 21.11.2012 bis 14:00 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 (per Email 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 7: (H) Buffer-/Heap-Overflows & Rootkits

Angreifer nutzen oftmals Schwachstellen in lokal installierten Applikationen.

a. Erläutern Sie knapp, was bei einem Buffer-Overflow genau passiert.

b. Betrachten Sie den folgenden Shellcode, der bei einem Buffer-Overflow ausgeführt werden soll. Welche Probleme könnten hierbei auftreten?

```
char shellcode[] = "\xbb\x14\x00\x00\x00"
                   "\xb8\x01\x00\x00\x00"
                   "\xcd\x80";
```

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

d. Ein Angreifer versucht meist durch Ausnutzen eines Buffer-Overflows die Programmauführung gezielt zu manipulieren. Zu welchem weiteren Zweck können speziell Heap-Overflows eingesetzt werden?

e. Man unterscheidet grundsätzlich zwei Typen von Rootkits: User-Mode- und Kernel-Mode-Rootkits. Erläutern Sie diese kurz.

f. Wie beurteilen Sie die Erkennung von Rootkit-Software durch eine signatur-basierte Anti-Virus-Software. Würde der Einsatz einer heuristischen (Anomalie-basierten) Erkennung helfen?

Aufgabe 8: (H) crypt & Passwort-basierte Authentifizierung

Bei älteren Unix-Systemen werden Nutzerpasswörter per *crypt* verschlüsselt gespeichert.

a. Welche Punkte der folgenden Beschreibung sind falsch? Korrigieren Sie den Text entsprechend.

   In einem Unternehmen übernimmt das Anlegen eines neuen Nutzerkontos der Administrator (root). Initial legt dieser auch das Passwort für den neuen Nutzer fest. Beim ersten Login wird der Nutzer nun aufgefordert, das Passwort zu ändern. Der Nutzer root ist aber auch nach dieser Änderung in der Lage, das per crypt und damit per AES verschlüsselte und in der Datei /etc/passwd gespeicherte Nutzerpasswort zu entschlüsseln. Um Wörterbuch-Attacken zu erschweren, wurde ein Salt eingeführt, der insgesamt 32 Bit lang ist. Der Salt bildet die ersten 4 Ziffern im verschlüsselten Passwort, welches als 32 Bit langer String gespeichert ist. Die Verschlüsselung von crypt ist auch bei heutiger Rechenleistung als sicher zu bezeichnen.

b. Oftmals findet sich in der Datei /etc/passwd statt des verschlüsselten Passwort-Strings der Wert *x*. Was bedeutet dieser Wert und welchen Vorteil hat dieser gegenüber der herkömmlichen Methode?

c. Welche Regeln empfehlen Sie für die Wahl eines guten Passwortes?