Technische Universität Berlin Fachgebiet Kommunikations- und Betriebssysteme Sommersemester 2014	**Aufgabenblatt 1** zu Grundlagen der Rechnersicherheit Dr.-Ing. Jörg Schneider, Frederick Hirsch

Aufgabe 1 abzugeben bis 23. April 2014 23:55h
Aufgabe 2 abzugeben bis 07. Mai 2014 23:55h

Die Abgabe der Übungsblätter erfolgt über ISIS bis 23:55 Uhr des jeweils festgelegten Abgabetages. Von jeder Gruppe wird die jeweils letzte Abgabe gewertet. In der Regel soll die Bearbeitung der Aufgaben als Datei abgegeben werden. **Einzig mögliches Abgabeformat ist hierbei PDF.** Andere Dateiformate oder Archivdateien werden **nicht** akzeptiert. Verspätete oder falsch formatierte Abgaben werden nicht bewertet. Die Abgaben werden nicht benotet, müssen allerdings erkennbar sinnvoll bearbeitet sein. Der Inhalt der Aufgaben wird in der jeweils folgenden Übung besprochen.

Aufgabe 1.1: Begriffe

a) Finden Sie je drei Beispiele aus der EDV-Praxis sowie eines aus einem anderen Gebiet für Safety und Security.

b) Geben Sie für zwei der Beispiele aus a) je zwei Schutz- und Sicherheitsmaßnahmen an.

Aufgabe 1.2: IT-Grundschutzhandbuch

Schauen Sie sich die IT-Grundschutz-Kataloge des BSI (www.bsi.de) vor der Übung an. Wie sind die Kataloge organisiert? Suchen Sie eine Gefährdung heraus, die Sie bisher regelmäßig in der Praxis berücksichtigen sowie eine, die für Sie bisher unbekannt bzw. nicht relevant war.

Aufgabe 1.3: Viren

Der Mailwurm Love Letter verbreitete sich im Jahr 2000 ziemlich schnell im gesamten Internet. Versuchen Sie detaillierte Informationen über den Wurm selber und seine Verbreitung herauszufinden.

a) Wie funktioniert der Wurm?

b) Wie erreicht der Wurm, dass er langfristig auf dem infizierten Rechner verbleibt und regelmäßig aktiviert wird?

c) Wie findet der Wurm den Weg zu weiteren Rechnern?

Bewerten Sie die eingesetzten Techniken aus heutiger Sicht. Falls Sie Schwachstellen in der Architektur identifizieren konnten, überlegen Sie, inwieweit aktuelle Viren diese Schwachstellen überwunden haben.

Hinweis: Sollten Sie dazu den Wurm selber untersuchen, stellen Sie durch geeignete Gegenmaßnahmen sicher, dass er nicht ausgeführt wird und Ihren oder anderer Rechner infiziert.

Aufgabe 2.1: Unsichere Software

a) Es ist bekannt geworden, dass auf dem Rechner bolero.cs.tu-berlin.de auf Port 12012 ein Server zum Austausch von geheimen Mitteilungen läuft. Die Authentisierung erfolgt mit Usernamen und Einmal-Passwort, die unverschlüsselt übertragen werden. Ein Teil der Authentisierungskomponente des Servers ist bekannt geworden. Leider sind nur drei der SMS mit dem Code angekommen.

```
#include <sys/socket.h> #include <netinet/in.h>
#include <time.h> #define LISTENPORT 12012 #define
MAXLINELEN 128 #define PASSLEN 32 void passwd_gen(char
*pass) {int i;
```

```
return; } int main(int argc, char **argv) {int s; int
client; struct sockaddr_in addr; socklen_t
addrlen;char *str,*str2; FILE *sock;char
password[PASSLEN];char line[MAXLINELEN];
```

```
;read(client,line,MAXLINELEN);if (strncmp (line,"USER
ALICE",10)) {fclose (sock);close
(client);continue;}fflush (sock);fprintf(sock,"%s␣OK,
SEND␣PASSWORD\n",line);
```

Untersuchen Sie die Code-Fragmente auf Schwachstellen und entwickeln Sie eine Vorgehensweise um die hinterlegte Nachricht auch ohne vorherige Kenntnis des Passwortes empfangen zu können. Geben Sie die hinterlegte Nachricht an, wenn Sie erfolgreich waren.

b) Auf ISIS ist ein CGI-Skript in Perl hinterlegt. Finden Sie möglichst viele Schwachstellen in diesem Skript. Geben Sie zu jeder Schwachstelle an, wie sie ausgenutzt werden kann, welche Gefahr für den Nutzer oder Betreiber daraus entstehen und wie sie behoben werden kann.

c) Stellen Sie zwei bekannt gewordene Schwachstellen in verbreiteten Anwendungen vor. Geben Sie an, wie das ungeplante Verhalten hervorgerufen werden kann, welche Gefahren daraus entstehen und bewerten Sie die vorgeschlagenen Schutzmaßnahmen bzw. Behebungen. Untermauern Sie, wenn möglich, Ihre Aussagen mit Quelltextausschnitten.

Aufgabe 2.2: Risiko und Sicherheitskonzept

a) Entwickeln Sie eine Schwachstellenanalyse und Bedrohungsanalyse für folgende Fälle:

- Modifizierung der Webseiten der Fakultät IV
- Unbefugtes Anmelden bei einem Webmail-Dienst
- Ausfall des Dateiservers einer kleineren Abteilung

b) Für ein kommerzielles Entwicklungslabor und eine Wohngemeinschaft soll ein Sicherheitskonzept aufgestellt werden. Welche Unterschiede in den Grundsätzen des Konzeptes würden Sie erwarten?

Hacking Tips: Buffer Overflow

Hier gibt es immer ein paar praktische Bastelaufgaben unterschiedlicher Schwierigkeit im Umfeld der behandelten Themen. Die Aufgaben sollen Anregungen für ein praktisches Auseinandersetzen mit dem Thema sein und sind nicht Teil des Kurses.

a) Schreiben Sie ein Programm, das durch Buffer Overflow oder Code Injection (Shell, SQL, include) verwundbar ist, oder nehmen Sie eine alte Version einer bekannt schwachen Software. Versuchen Sie dann darüber eigenen Programmcode auszuführen oder das Programm zum Absturz zu bringen.

b) Untersuchen Sie den Patch für die Heartbleed-Lücke in OpenSSL. Versuchen Sie nachzuvollziehen wie der Fehler ausgenutzt wird und welcher Schaden entsteht.
Installieren Sie eine ungepatchte OpenSSL-Version 1.0.1f und versuchen Sie die Lücke selbst auszunutzen. Welche Daten können Sie lesen? Wie aufwändig ist das Ausnutzen dieser Lücke?