Übungsaufgabe #5: Sicherheitslücken finden und ausnutzen

20.1.2010

In dieser Aufgabe sollen Sicherheitslücken in einem vorgegebenen Programm gefunden und ausgenutzt werden. Das Programm ist unter `/proj/syssec/bin/abgabe` zu finden, der Sourcecode unter `/proj/syssec/bin/abgabe.c`. Das kompilierte Binary wurde mit dem Debian Etch gcc (der Standard-compiler im CIP-Pool) ohne Optimierungen übersetzt und mit set userid auf den Benutzer `syssec` abgelegt:

```
$ ls -l /proj/syssec/bin/abgabe
-r-sr-xr-x 1 syssec cipguest 8846 Jan 16  2008 /proj/syssec/bin/abgabe
```

Die eigentliche Aufgabe des Programms besteht darin, eine einfache Übungsabgabe zu implementieren, bei der das Abgabeprogramm einen durch den Benutzer gegebenen C-Quelltext übersetzt und in einem privaten Abgabeverzeichnis (`/proj/i4syssec/a5/abgabe/`) ablegt. Dieses Verzeichnis ist nur für den syssec-Benutzer zugreifbar.

Durch schlechte Programmierung finden sich in diesem Programm jedoch mehrere Sicherheitslücken, welche verschieden schwer ausgenutzt werden können. In dieser Übungsaufgabe sollen so viele Sicherheitslücken wie möglich gefunden und genutzt werden, um eigene Befehle unter der Benutzerkennung "`syssec`" auszuführen. Nach dem erfolgreiche Ausnutzen der ersten Sicherheitslücke soll eine Datei mit den Logins der Gruppenmitglieder als Dateiname im Verzeichnis `/proj/i4syssec/a5/exploited/` angelegt werden (z.B. `/proj/i4syssec/a5/exploited/gernoth_tartler`). In diesem Verzeichnis bitte keine Dateien löschen. Die anderen Sicherheitslücken sollen in den Abgabeübungen gezeigt und (wenn erfolgreich) vorgeführt werden.

Die Abgabe der bearbeiteten Aufgabe erfolgt in den Übungen am 10. oder 12.2. Die Bearbeitung kann in Gruppen zu zwei oder drei Personen erfolgen.