michael.engel [☺] hs-coburg.de

Praktikum zur Vorlesung
Malware-Analyse und Reverse Engineering
Sommersemester 2017

Praktikumsaufgabe 3

Besprechung am Donnerstag, 20. April 2017

Hinweise: Praktikumsaufgaben müssen in der vorgegebenen Zeit in den eingeteilten Gruppen bearbeitet werden. Die Lösung der Aufgaben wird bewertet, jedes Gruppenmitglied soll Fragen zu den einzelnen Aufgaben beantworten können. Bei Unklarheiten und Rückfragen wird selbstverständlich eine Hilfestellung gegeben.

3.1 Buffer overflows

Experimentieren Sie mit Buffer overflows, indem Sie den Kontrollfluss eines Programms verändern.

- Schreiben Sie ein Programm, das folgende Funktionen enthält:
  a. Eine Funktion `a`, die einen Text ausgibt (z.B. “HACKED!!”) und danach mit der Systemfunktion `execl` ein Programm aufruft (z.B. `/bin/date`).
  b. Eine Funktion `b`, die ein char-Array fester Länge (z.B. 8 Zeichen) alloziert und eine der in der Vorlesung erwähnten *unsicheren* libc-Funktionen (z.B. gets) verwendet, um einen Buffer overflow herbeizuführen
  c. Eine Funktion `main`, die die Adresse der Funktion `a` ausgibt und anschließend die Funktion `b` aufruft.
- Übersetzen Sie Ihr Programm mit der in der Vorlesung genannten Compileroption `-fno-stack-protector`
- Erzeugen Sie einen Buffer overflow, der das Programm zum Absturz bringt (segmentation fault) und verifizieren Sie mit Hilfe von gdb die fehlerhafte Rücksprungadresse Sie können einen Text als Eingabe an das Programm übergeben, indem Sie in der Shell folgende Befehle aufrufen:

  ```
  echo -e '1234567812345678\xaf\xfe\xde\xad' | ./prog
  ```

  Wie Sie sehen, können auch Hexadezimalzeichen einfach erzeugt werden.
- Erzeugen Sie einen Buffer overflow, der den Programmfluss so umleitet, dass durch den Buffer overflow die Funktion `a` aufgerufen wird.

Zu Parametern von Systemfunktionen usw. können Sie mit dem Befehl `man funktionsname` eine Hilfeseite anzeigen. Einige Namen von Systemfunktionen sind auch als Befehle im System vorhanden, damit zeigt man evtl. die falsche Hilfeseite an. In diesem Fall `man 2 funktionsname` oder `man 3 funktionsname` probieren.
Wenn gdb in Ihrer Linux-Umgebung noch nicht installiert ist, können Sie diesen mit `sudo apt-get install gdb` nachinstallieren.