michael.engel [☺] hs-coburg.de

Praktikum zur Vorlesung
Malware-Analyse und Reverse Engineering
Sommersemester 2017

Praktikumsaufgabe 2

Besprechung am Donnerstag, 6. 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.

2.1 Hacken!

Linux erlaubt es, shared libraries zu überladen, also Funktionen einer standardmäßig vom dynamischen Linker geladenen Library durch eigene Funktionen zu ersetzen.
Dies erfolgt mit Hilfe der Umgebungsvariablen `LD_PRELOAD`. Diese Funktionalität kann verwendet werden, um einem binären, dynamisch gelinkten Programm unerwünschte Funktionalität “unterzuschieben”.

- Schreiben Sie ein C-Programm, das mit Hilfe der Funktion `rand` 10 Zufallszahlen zwischen 0 und 99 (inklusive) erzeugt und ausgibt.

  Initialisieren Sie den Zufallszahlengenerator mit der Funktion `srand(time(NULL));` auf einen “zufälligen” Anfangswert (*seed*) – die aktuelle Zeit in Sekunden seit dem 1.1.1970.

  Übersetzen Sie Ihr Programm mit gcc und überprüfen Sie, dass Zufallszahlen generiert werden.

- Schreiben Sie eine eigene C-Funktion `rand` in einer Datei `unrandom.c`, die eine konstante Zufallszahl (z.B. 42) zurückgibt und übersetzen Sie diese als shared library mit `gcc -shared -fPIC unrandom.c -o unrandom.so`

- Injizieren Sie Ihre Funktion, indem Sie vor dem Aufruf Ihres Zufallszahlengenerators die Umgebungsvariable `LD_PRELOAD` in der bash-Shell setzen: `export LD_PRELOAD=$PWD/unrandom.so`

  Wie sehen Ihre Zufallszahlen jetzt aus?

- Suchen Sie sich ein beliebiges Binärprogramm (z.B. aus den Verzeichnissen /bin oder /usr/bin) und ersetzen Sie darin einen Funktionsaufruf durch eine mit `LD_PRELOAD` überladene eigene Funktion. Da üblicherweise keine Symbole in den Programmen mehr enthalten sind, versuchen Sie, den Sourcecode des Programms zu finden und dort eine “interessante” Funktion zu ersetzen (z.B. localtime in /bin/date).