Lehrstuhl für Systemsicherheit
Prof. Dr. Thorsten Holz
Andre Pawlowski

Vorlesung Betriebssystemsicherheit
Wintersemester 2014/2015
Ruhr-Universität Bochum

4. Übung

19. Dezember 2014
Abgabe der Hausaufgaben: per Moodle bis zum 12. Januar 2015, 16 Uhr
Bei Fragen und Problemen können Sie sich per E-Mail/Moodle an die Betreuer wenden.

Bitte lösen Sie alle Linux-Aufgaben in der xubuntu-VM aus der letzten Übung.

Aufgabe 1 (vuln.c) (4 Punkte)

Bitte benutzen Sie nur die bereitgestellten Dateien `vuln.c` und `vuln` aus dem Ordner `Aufgabe1`. Bitte kompilieren Sie das Programm nicht neu.

Aufgabe 1.1 – Exploiting

Nutzen Sie die Schwachstelle im Programm `vuln.c` aus, um durch Übergabe eines entsprechenden Kommandozeilenparameters eine Shell zu erzeugen. Den Shellcode können Sie dabei beliebig wählen. Bitte achten Sie darauf, dass der Exploit stabil läuft, d.h. auch nach dem Reboot des Systems funktioniert.

Schreiben Sie den Exploit als kleines Programm, das `vuln` aufruft und laden Sie den Quelltext bei Moodle hoch. Beschreiben Sie außerdem kurz als Kommentar im Quelltext, wie Ihr Exploit funktioniert. Um Probleme beim Korrigieren durch verschobene Adressen vorzubeugen, gehen wir davon aus, dass sich die Datei `vuln` im Ordner `/home/user/aufgabe1` befindet und auch der Exploit aus diesem Ordner heraus ausgerufen wird.

Aufgabe 1.2 – CFI

Wäre die Ausnutzung der Schwachstelle auch mit CFI (*Control Flow Integrity*) möglich oder verhindert CFI Ihren Exploit? Erläutern Sie kurz Ihre Lösung.

Aufgabe 1.3 – Fixing

Wie kann die Schwachstelle im Code verhindert werden? Geben Sie den kommentierten Quellcode Ihrer Lösung ab, der diese Schwachstelle behebt.

Aufgabe 2 (Confinement Problem) (1 Punkt)

Aufgabe 2.1

Erläutern Sie in maximal zwei Sätzen das Confinement Problem.

Aufgabe 2.2

Nennen Sie beide Typen von Covert Channels und erläutern Sie in je maximal zwei Sätzen das zugrundeliegende Problem.

Aufgabe 2.3 – Leseaufgabe (Bonus, keine Bewertung)

Lesen Sie sich das Paper „Evaluating SFI for a CISC Architecture“ von McCamant und Morrisett (Usenix Security Symposium 2006, http://groups.csail.mit.edu/pag/pubs/pittsfield-usenix2006.pdf) durch.