PRÄSENZ

BUFFER OVERFLOWS UND DEREN FOLGEN

HACKING: BINARY EXPLOITATION

Die Herausforderung: Neue Angriffsszenarien im Zuge steigender Vernetzung. Unternehmen müssen heutzutage ihre Systeme in adäquater Weise absichern. Trotz vorhandener Schutzmechanismen, wie z. B. durch nicht ausführbare Speicherregionen, Randomisierung von Adressen oder durch den Compiler eingefügte Stack Cookies, werden Schwachstellen in Anwendungen dennoch erfolgreich ausgenutzt. In diesem Seminar lernen Sie, wie Sie sich auf derartige Angriffe vorbereiten. Gerade der Bereich Binary Exploitation steht dabei im Fokus. Geben Sie Hackern keine Chance!

Inhalte des Seminars

Tag 1

- Grundlagen Buffer Overflows, Debugging, Dissassembler
- Praktische Übung: Debuggen und Reverse Engineering
- Einführung in die Thematik des Stacks
- Praktische Übung: Erster Exploit ohne Schutzmaßnahmen

Tag 2

- Schutzmaßnahmen durch Compiler
- Praktische Übung: Exploit mit Compilerschutzmaßnahmen
- Schutzmaßnahmen durch System
- Praktische Übung: Exploit mit Systemschutzmaßnahmen

Tag 3

- Einführung in die Thematik des Heaps
- Praktische Übung: Exploit ohne Schutzmaßnahmen
- Praktische Übung: Exploit mit Schutzmaßnahmen (optional)

Ihr Nutzen

» Nach dem Seminar können Sie das Vorgehen eines Hackers nachvollziehen und Exploits zum Aufzeigen der Schwachstelle entwickeln.

» Sie kennen typische Programmierfehler in C-Code und die Grenzen der Schutzmechanismen.

» Sie können die Anwendbarkeit der Schutzmechanismen für die eigene Entwicklung einschätzen.

INFORMATIONEN IM ÜBERBLICK

Basiswissen Linux: Routinierter Umgang mit der Bourne-Again Shell (BASH) und GNU Debugger (GDB); Programmierkenntnisse: Flüssiges Lesen und Verstehen von C-Code; Programmiererfahrung mit C oder Python Assembler: x86_64 Assembler lesen und verstehen.

Mitarbeitende, die bei Entwicklung, Testen, Betreiben oder Anwendung das Vorgehen eines Hackers kennenlernen wollen, um mithilfe dieser Erkenntnisse die Sicherheit ihrer Systeme zu verbessern.

3 Tage Präsenz

1800,–

Weiden in der Oberpfalz

Veranstaltet durch

Fraunhofer AISEC

Referent:

Tilo Fischer, wiss. Mitarbeiter Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/binary-exploitation