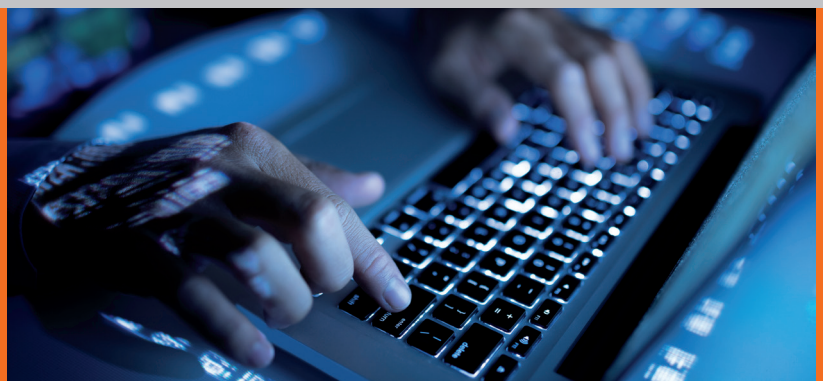
Fraunhofer
ACADEMY

SEMINAR



IHRE VORTEILE AUF EINEN BLICK

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

… typische Programmierfehler in C-Code erkennen und die Grenzen der Schutzmechanismen verstehen.

… die Anwendbarkeit der Schutzmechanismen für die eigene Entwicklung einschätzen.

Dieses Seminar bietet Ihnen…
…einen tiefen Einblick in ausgewählte Techniken von Binary Exploitation.

… praktische Umsetzung von Methoden zur Umgehung von Schutzmechanismen und Entwicklung von eigenen Exploits.

Melden Sie sich gleich an!
www.academy.fraunhofer.de/binary-exploitation

HACKING: BINARY EXPLOITATION

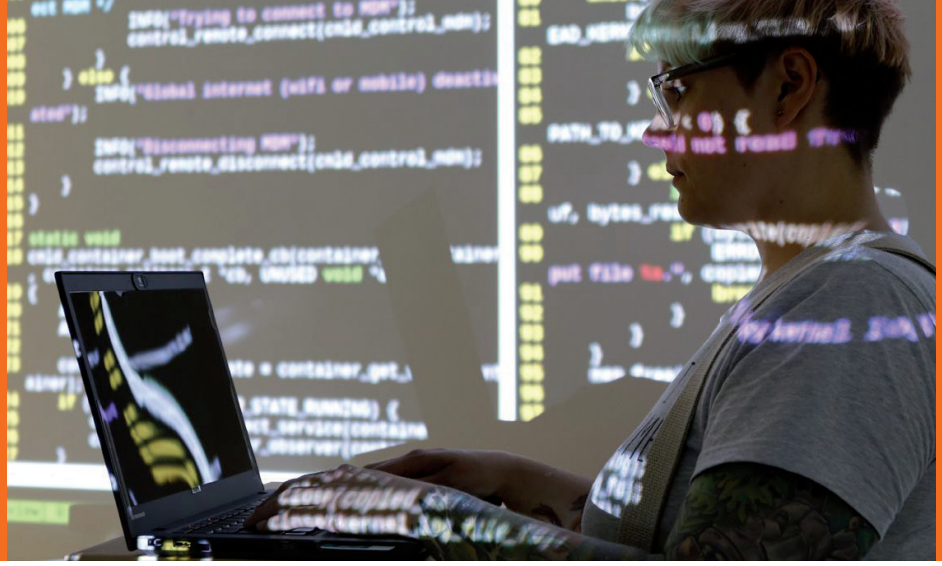
Buffer-Overflows und deren Folgen

Die Herausforderung: Neue Angriffsszenarien im Zuge steigender Vernetzung

Immer mehr Geräte und Systeme sind heute über das Internet und andere Netzwerke erreichbar und direkten Angriffen ausgesetzt. Dies stellt viele Unternehmen vor die Herausforderung, ihre Systeme geeignet abzusichern, um mögliche Angriffe von Hackern abzuwehren. Trotz vorhandener Schutzmechanismen – wie z.B. durch nichtausführbare Speicherregionen, Randomisierung von Adressen oder durch den Compiler eingefügten Stack-Cookies – werden Schwachstellen in Anwendungen dennoch erfolgreich ausgenutzt. Dadurch stellt sich die Frage, wie diese Schutzmechanismen durch die Angreifer umgangen werden.

Die Lösung: Binary Exploitation aus Sicht der Hacker verstehen und zuvorkommen

Im Rahmen dieses Seminares erlernen die Kursteilnehmenden die Vorgehensweise von Hackern, um besser auf derartige Angriffe vorbereitet zu sein. Der Schwerpunkt dieses Seminars liegt dabei im Bereich Binary Exploitation, also: Wie können beispielsweise Programmierfehler in C-Code ausgenutzt werden, um fremden Code einzuschleusen und auszuführen? Dabei wird auch die Frage beantwortet, wie effektiv die System- und Compiler-Schutzmechanismen greifen, und wie und unter welchen Umständen die Angreifer diesen Schutz umgehen können.



INFORMATIONEN IM ÜBERBLICK

Kurs: Hacking: Binary Exploitation
Voraussetzungen: 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
Dauer: 3 Tage in Präsenz **Kurssprache:** Deutsch **Teilnehmerzahl:** max. 10 Teilnehmer **Veranstaltungsort:** Weiden in der Oberpfalz / Garching bei München

Kosten: 1.800 €

Veranstaltet durch:

Fraunhofer AISEC

UNSERE REFERENTEN

Tilo Fischer
Wissenschaftlicher Mitarbeiter Sichere Betriebssysteme, Fraunhofer AISEC

Die Inhalte: Exploitation in Theorie und Praxis

- Grundlagen BufferOverflows, Debugging, Dissassembler
- Praktische Übung: Debuggen und reverse engineeren
- Einführung in die Thematik des Stacks
- Praktische Übung: Erster Exploit ohne Schutzmaßnahmen

- Schutzmaßnahmen durch Compiler
- Praktische Übung: Exploit mit Compiler-schutzmaßnahmen
- Schutzmaßnahmen durch System
- Praktische Übung: Exploit mit System-schutzmaßnahmen

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

Die Lernziele: Schwachstellen erfolgreich identifizieren

- Identifikation typischer Programmier-fehler in der Sprache C
- Erkennen der Grenzen von vorhandenen Schutzmechanismen
- Tiefgründige Kenntnisse über Speicher-architekturen
- Erlernen von Methoden zur Umgehung von Schutzmechanismen
- Erstellen von Exploits zur Ausnutzung von Schwachstellen in Applikationen

Die Zielgruppe: Entwickler, Tester, Betreiber und Anwender

Mitarbeiterinnen und Mitarbeiter, die als Entwickler, Tester, Betreiber oder Anwender das Vorgehen eines Hackers kennenlernen wollen, um mit Hilfe dieser Erkenntnisse die Sicherheit ihrer Systeme zu verbessern.

Das Lernlabor Cybersicherheit: Weiterbildung für die IT-Sicherheits-experten von morgen

Das Lernlabor Cybersicherheit ist eine Zusammenarbeit zwischen Fraunhofer und ausgewählten Fachhochschulen, um aktuelle Erkenntnisse auf dem Gebiet der Cybersicherheit in Weiterbildungsangebote für Unternehmen zu überführen. Fach- und Führungskräfte aus Industrie und öffentlicher Verwaltung erhalten an zahlreichen Standorten in Deutschland eine kompakte Qualifizierung in hochwertigen Laboren mit aktueller IT -Infrastruktur.

HABEN SIE NOCH FRAGEN ZU…

… Binary Exploitation und sicheren Betriebssystemen?
Tilo Fischer
Fraunhofer AISEC
Telefon +49 89 3229986-201
tilo.fischer@aisec.fraunhofer.de

… Anmeldung, Organisation oder weiteren Angeboten?
Adem Salgin | Fraunhofer Academy
Telefon +49 89 1205-1555
cybersicherheit@fraunhofer.de