Einführung in die Firmwareanalyse

Seminar zu Firmware-Extraktion und initialer Analyse

Erlernen Sie Methoden zur Firmwareanalyse, um Sicherheitslücken zu erkennen. Der Kurs vermittelt Reverse Engineering, statische und dynamische Analysemethoden und praxisnahe Übungen. Ideal für IT-Sicherheitsexperten und Analyst:innen, die ihre Kenntnisse im Umgang mit Firmware vertiefen möchten.

Praxisnahe Einführung in die Analyse und Absicherung von Firmware

Mit der zunehmenden Vernetzung durch IoT und Industrie 4.0 wächst die Bedrohung durch Angriffe auf Firmware – die Software, die eingebettete Systeme steuert. Manipulierte oder unsichere Firmware kann das Verhalten von Geräten verändern und als Angriffsvektor in Netzwerke dienen.

Um Sicherheitsrisiken zu minimieren, ist es entscheidend, Firmware zu analysieren und Schwachstellen zu erkennen. Das Seminar vermittelt eine Einführung in die Firmwareanalyse.

Sie lernen, Firmware zu extrahieren, zu entschlüsseln und zu analysieren, um Schwachstellen und Manipulationen aufzudecken. Es werden statische und dynamische Analysemethoden vorgestellt, darunter Reverse Engineering und die Nutzung spezialisierter Analysewerkzeuge.

Kursdetails auf einen Blick

- Für **Analyst*innen. Reverser*innen, IT-Forensiker*innen**
- **Inhouse Training**
- Dauer: **2 Tage**
- Format: **Präsenz**
- Kosten: 1.200,00 Euro (zzgl. MwSt.)

Firmware-Sicherheit praxisnah erlernen und eigenständig anwenden

Praktische Übungen bilden einen zentralen Bestandteil des Seminars und unterstützen die Teilnehmenden dabei, die zuvor erworbenen Kenntnisse direkt in die Praxis umzusetzen. Schritt für Schritt lernen sie, typische Sicherheitslücken in Firmware zu erkennen und einzuordnen. Der Schwerpunkt liegt dabei stets auf realen Beispielen und praxisnahen Szenarien, die typische Herausforderungen aus dem Berufsalltag widerspiegeln. Auf diese Weise wird ein solides und nachhaltiges Verständnis für die besonderen Sicherheitsrisiken im Bereich Firmware vermittelt.

Das Seminar richtet sich an IT-Sicherheitsfachkräfte, Analyst:innen sowie Forensiker:innen, die bereits über Grundkenntnisse in Linux, Programmierung und Betriebssystemen verfügen. Sie erhalten die Möglichkeit, ihre Fähigkeiten systematisch zu vertiefen und mit konkreten Methoden der Firmwareanalyse zu verbinden. Nach Abschluss sind die Teilnehmenden in der Lage, Firmware zu untersuchen, Schwachstellen zu identifizieren und Angriffsflächen einzuschätzen.

Nach dem Seminar können Sie:

- **Firmware** aus den meisten Geräten **extrahieren**
- Initiale, toolgestützte **Analysen von Firmware durchführen**
- Einschätzen, wie viel Sorgfalt der Hersteller bei der Entwicklung der Firmware walten ließ.
- Technische oder organisatorische **Maßnahmen ergreifen** um identifizierte **Schwachstellen einzudämmen.**

Alle Kursdetails und die Anmeldung finden Sie hier:

https://s.fhg.de/Firmware-Extraction

Kursinhalte

Das Spektrum der behandelten Themen umfasst:

- Beschaffung von Firmware über Hersteller oder Geräteschnittstellen
- Extraktion der Firmware vom Gerät mittels Hardware-Werkzeugen
- Entpacken der Firmware-Container, um einzelne Komponeten wie Web- oder Samba-Server zu identifizieren
- Analyse der Firmware-Komponenten anhand statischer und dynamischer Analysemethoden
- Einführung in die Benutzung der wichtigsten Werkzeuge für Firmware-Extraktion und -Analyse

Zugangsvoraussetzung:

Grundkenntnisse im Umgang mit Linux und der Kommandozeile.

Fachlicher Ansprechpartner am Fraunhofer FKIE

Johannes von Dorp
Tel. +49 228 50212-570
johannes.vom.dorp@fkie.fraunhofer.de

Fraunhofer FKIE
Zanderstraße 5
53177 Bonn

Lernlabor
Cybersicherheit