HMTS
HM Training Solutions

INDEPENDENT • INNOVATIVE
INTERNATIONAL

M 67

Ein neuer Workshop

IoT Hacking 101

Lernen von den Profis –
Ihre Trainer sind Dennis Heinze und Frieder Steinmetz.

Der Kurs beinhaltet ein Hardware Hacking Tool namens Tigard, das verschiedenste Schnittstellen und Protokolle im IoT-Bereich beherrscht sowie einen Logic Analyzer zur Analyse von Hardware-Schnittstellen. Für einige Übungen stellen Ihnen die Referenten einen Rasperry Pi Pico zur Verfügung. **Damit Sie auch nach Workshopende weiter trainieren können, dürfen Sie alles mit nach Hause nehmen.**

Kursbeschreibung

IoT-Geräte sind äußerst vielseitig. Sie nutzen eine Vielzahl von physikalischen Schnittstellen, Protokollen und Software. Zudem sind sie oft in größere (Cloud-) Ökosysteme eingebunden. Unser Workshop "IoT Hacking 101" bietet einen fundierten Einstieg in das Thema IoT-Hacking.

**Während des Workshops werden allgemeine Aspekte von IoT-Geräten behandelt, wobei der Schwerpunkt auf einem praktischen Beispiel liegt.
Die Teilnehmer erhalten ein echtes, auf dem Markt verfügbares IoT-Gerät, an dem Testmethoden und Schwachstellen veranschaulicht und erprobt werden.**

Aufgrund der umfangreichen und vielfältigen Natur des Themas legen wir den Schwerpunkt im Workshop auf praktische Übungen anstelle von rein theoretischem Inhalt. Dabei werden nicht alle Aspekte, wie Protokolle oder Technologien, bis ins kleinste Detail theoretisch behandelt. Der Workshop bietet jedoch ausreichend Raum für Fragen und Erläuterungen, um Teilnehmer mit unterschiedlichem Hintergrund abzuholen.

5. – 7. November 2024, Heidelberg

Diese Veranstaltung wird als Weiterbildung bei Rezertifizierungsmaßnahmen von verschiedenen Instituten anerkannt.

HM Training Solutions, Falkenstraße 6 · D-63820 Elsenfeld
Telefon +49 (0) 6022 508 200,Fax +49 (0) 6022 508 9999
E-Mail: info@hm-ts.de – Internet: https://www.hm-ts.de

IoT Hacking 101

M 67

Ein neuer dreitägiger Kurs in deutscher Sprache

Seminarinhalt

Kursinhalte erster Tag

Einführung
Background und Reconnaissance
Threat Modeling und Attack Surface
Active Recon

Kursinhalte zweiter Tag

Network Hacking
Hardware Hacking
Firmware Hacking

Kursinhalte dritter Tag

Firmware Hacking
Wireless Hacking
Infrastruktur und Cloud
Zusammenfassung

Warum Sie diesen Kurs besuchen sollten

IoT-Geräte sind allgegenwärtig. Aufgrund ihrer Vielfältigkeit und Komplexität sind jedoch viele dieser Geräte nicht auf einem akzeptablen Stand, was die IT Sicherheit betrifft. Wenn Sie sich für das Thema IoT-Hacking interessieren, bietet dieser Workshop die ideale Einführung anhand praktischer Beispiele. Durch die Möglichkeit, an einem echten IoT-Gerät zu üben, erhalten Sie zudem praxisnahe Erfahrungen, die Sie bei einer möglichen Sicherheitsanalyse direkt anwenden können.
Auch im privaten Bereich, zum Beispiel bei Smart Home Produkten, sollten Sie nach dem Workshop die Kenntnisse besitzen um festzustellen, ob ein Produkt Mindeststandards im Bereich Security aufweist.

HM TRAINING SOLUTIONS ON-SITE SERVICE

Alle HM Training Solutions Seminare stehen auch firmenintern zur Verfügung. Sie können auf den Bedarf Ihrer Organisation zuge schnitten werden. Weitere Details erhalten Sie unter der Telefonnummer +49 (0) 6022 508 200.

IoT Hacking 101

M 67

Ein neuer dreitägiger Kurs in deutscher Sprache

Teilnehmervoraussetzungen

Dieser Workshop setzt keine Kenntnisse im Penetration Testing voraus.
Wir beginnen mit den Basics des IoT Hacking. Neugierde und eventuelle Erfahrungen im Bereicht IT Security sind hilfreich, aber nicht notwendig.

Voraussetzungen:

- Grundlegende Kenntnisse von Linux/ Unix-basierten Systemen und Netzwerken
- Grundlegende Kenntnisse in der Verwendung der Kommandozeile
- Grundlagen im Penetration Testing oder Programmierung sind hilfreich, aber optional
- Ein Laptop mit root/admin-Rechten
- Die Möglichkeit eine virtuelle Maschine zu verwenden. Präferiert VirtualBox, andere Technologien sind auch möglich. Größe der VM ca. 40GB. Die VM enthält bereits die für die Übungen benötigte Software.

Zielgruppen

- ITler, die sich in Richtung IoT Pentesting entwickeln wollen
- IoT Entwickler, die mehr über IoT Security lernen wollen
- Alle anderen, die an IoT Hacking interessiert sind

IoT Hacking 101

M 67

Ein neuer dreitägiger Kurs in deutscher Sprache

Profile der Seminarleiter

Ihr Trainer, Frieder Steinmetz erwarb seinen Master in Informatik-Ingenieurwesen mit Fokus auf Sicherheit eingebetteter Geräte an der Technischen Universität Hamburg. Er hat einen Hintergrund in theoretischer Kryptographie und veröffentlichte Arbeiten zur praktischen Sicherheit verschlüsselter Messaging-Protokolle und Angriffe über USB-Geräte. Heute arbeitet er als Security Analyst bei der ERNW GmbH. Seine Arbeit konzentriert sich auf das Pentesting von mobilen und eingebetteten Geräten sowie deren Back-End-Kommunikation und -Infrastruktur. Er gibt regelmäßig Schulungen zu Themen wie RFID / NFC-Hacking, Pentesting von Webanwendungen und Kommunikationssicherheit.

Dennis Heinze arbeitet als Security Analyst & Researcher bei der ERNW GmbH. Er erwarb seinen Master in IT-Sicherheit mit den Schwerpunkten Netzwerk- und Systemsicherheit an der TU Darmstadt. In der Vergangenheit beschäftigte er sich, unter anderem mit der Sicherheit der Bluetooth-Technologie. Dabei veröffentlichte er Arbeiten zur Untersuchung der Sicherheit und Implementierung von Bluetooth Protokollen im Apple Ökosystem. In seiner Arbeit bei ERNW liegt der Fokus auf dem Pentesting von mobilen und eingebetteten Geräten sowie deren Kommunikation und Back-End Systemen.

DETAILS ZUM ANMELDEFORMULAR

Drei Wege zur Anmeldung

Per Post: Bitte dieses Anmeldeformular ausfüllen und an HM Training Solutions senden.
Per E-Mail: **Info@hm-ts.de**
Per Webseite: https://www.hm-ts.de

Gebühren

4.590 €. + 19% MwSt.

Bestätigungsbrief

Ihre Anmeldung bestätigen wir per Mail oder Brief. Er enthält Details über die Veranstaltung, Ort, Anfangs- und Endzeiten. Mittagessen, Kaffeepausen (inkl. Begrüßungskaffee mit Snacks), ein Abendessen am ersten Abend und die Seminardokumentation sind im Preis enthalten.

Änderungen

HM Training Solutions behält sich das Recht vor, bei Eintreten nicht vorhersehbarer Umstände das Seminar räumlich und/oder zeitlich zu verlegen, einen anderen Referenten ersatzweise einzusetzen oder die Veranstaltung zu stornieren. Weitergehende Ansprüche bestehen nicht.

Stornierung seitens des Teilnehmers

Bitte reichen Sie Stornierungen schriftlich per Post oder Email (info@hm-ts.de), ein. Bestätigte Anmeldungen können bis zu sechs Wochen vor Seminarbeginn kostenfrei storniert werden, danach berechnen wir die gesamte Seminargebühr. Eine Übertragung an einen Ersatzteilnehmer ist jederzeit möglich.

Veranstaltungsort und Hotels

Ihre Anmeldebestätigung enthält Details zur Veranstaltungsadresse, in deren Nähe sich eine Reihe von Hotels in unterschiedlichen Kategorien befinden.

Firmeninterne Seminare

Alle Trainings von HM Solutions können auch firmenintern und zugeschnitten auf den Bedarf der jeweiligen Organisation durchgeführt werden. Weitere Informationen erhalten Sie unter der Telefon-Nr. +49 (0) 6022 508 200.

Die Teilnehmerzahl ist begrenzt. Wir berücksichtigen Ihre Anmeldung in der Reihenfolge des Eingangs.

ANMELDEFORMULAR

IoT Hacking 101

❒ **5. – 7. November 2024, Heidelberg**

❒ Bitte reservieren Sie _____ Platz/Plätze **zum Einzelpreis von 4.590 €** + 19% MwSt.

Wir senden Ihnen die Kursdokumentation als pdfs vor Kursbeginn zu!

Herr/Frau Vorname Nachname

Funktion

Firma

Adresse

Postleitzahl Ort

Land

Telefonnummer

Mobilfunknummer

E-Mail

Unterschrift

BUCHUNGSREFERENZ HM67

Zahlung

❒ Bitte um Rechnungsstellung

Rechnungsadresse (falls nicht identisch mit obiger Anschrift).

PO-Nummer

Zusätzliche Teilnehmer

1. Herr/Frau Vorname Nachname

Funktion

E-Mail

2. Herr/Frau Vorname Nachname

Funktion

E-Mail

3. Herr/Frau Vorname Nachname

Funktion

E-Mail