SEMINAR: HACK HARDWARE

Seminar für alle, die mit Hacker Hardware ihre Angriffs-Fähigkeiten erweitern wollen

DAS UNTERNEHMEN LOG(2) OHG

Pen Test in Hardware und Software. Enterprise Ressource Ninjas

Mit mehr als 25 Jahren internationaler Erfahrung in den USA, Asien und Australien mit renommierten großen Kunden und Partnern sind wir ein idealer Partner für alle neuen Sicherheitstechnologien.

Abwehr und Angriff, die beiden Seiten der Hacker Security, sind unsere Leidenschaft.

ENTDECKE DIE WELT DES HARDWARE HACKINGS: EIN INTENSIVER WORKSHOP FÜR IT-PROFIS

Hardware Hacking ist ein spannendes und oft unterschätztes Feld, das enormes Potenzial für IT-Sicherheitsexperten bietet. In unserem neuen Hacker Workshop bieten wir Ihnen die Möglichkeit, sich intensiv mit diesem Thema auseinanderzusetzen und gleichzeitig die dafür benötigten Tools direkt mit nach Hause oder ins Büro zu nehmen.

Unsere Idee für diesen Workshop entstand bei einem unserer letzten SAP-Hackerworkshops in Hamburg, veranstaltet von der IBS Schreiber GmbH. Obwohl eine Stunde dem Thema Hardware Hacking gewidmet war, wurde schnell klar, dass das Interesse der Teilnehmer weit darüber hinausging. Viele wünschten sich mehr Zeit und die Möglichkeit, die Werkzeuge direkt am Arbeitsplatz einsetzen zu können. Daher haben wir ein umfassendes Seminar konzipiert, das genau diese Bedürfnisse erfüllt.

WORKSHOP-HIGHLIGHTS: VIER INNOVATIVE TOOLS IM FOKUS

Wir als Sicherheitsunternehmen können entscheidend dazu beitragen, Unternehmen bei der Implementierung in die SAP-Cloud zu unterstützen. Durch die Kombination von Expertise in der Cybersicherheit, mit spezifischem Wissen über SAP-Lösungen kann log(2) eine nahtlose und sichere Migration in die SAP-Cloud ermöglichen.

„Alles ist praxiserprobt und wird in fast jedem unserer Pen Tests eingesetzt.
Oft präsentieren wir speziell die Tools den Kunden im Umfeld des Pen Tests.

Das schärft zusätzlich die Sicherheitswahrnehmung im Unternehmen.“

So erreichen Sie uns

log(2) oHG
Dorfstraße 90 A
17375 Hintersee

info@log2.de
https:\\www.log2.de
Unser Blog:
https:\\www.counterblog.org

RUBBER DUCKY

Der Klassiker unter den USB-Hacks: Der Rubber Ducky ermöglicht die Einspeisung von Skripten und SMB-Hacks, die mit einem Raspberry Pi realisiert werden können. Diese Techniken sind essenziell für jeden, der sich mit Penetrationstests und Sicherheitslücken in IT-Systemen auseinandersetzen möchte.

HAK5 PINEAPPLE

Das ultimative Tool zum Hacken von WiFi-Netzwerken, Terminals und Smartphones in Gäste- und Unternehmensnetzwerken. Der Pineapple wird oft in Penetrationstests eingesetzt, um die Sicherheitslücken in drahtlosen Netzwerken aufzudecken. Besonders berüchtigt ist der „Evil WiFi“ Knoten, der es ermöglicht, alle umgebenden Smartphones anzugreifen – ideal für die Sicherheitsbewusstseinsschärfung in Unternehmen.

FLIPPER ZERO

Erleben Sie die vielseitigen Möglichkeiten des Flipper Zero, ein Tool, das die Manipulation und das Kopieren von NFC-Kommunikation (wie Hotelkarten, Kasino-Karten und Mitarbeiter-Ausweisen) ermöglicht. Darüber hinaus bietet es erweiterte USB-Hacks, um aus Citrix-Sessions und RDP-Desktops auszubrechen. Der Flipper Zero allein ist ein unerschöpfliches Thema, das tiefere Einblicke in moderne NFC- und USB-Hacking-Techniken bietet..

SHARKJACK (HAK5)

Das universelle Tool für das schnelle Ausspionieren der gesamten Netzwerk-Architektur über ein Handy als Terminal. Besonders effektiv ist der Einsatz in Unternehmensumgebungen, zum Beispiel in Kopierer-Ecken. Der SharkJack ist ein Standard in Penetrationstests für umfassendes Netzwerk-Sniffing und bietet wertvolle Einblicke in die Netzwerksicherheit.

PRAXISORIENTIERTE SCHULUNG MIT DIREKTEM MEHRWERT

Das Beste an unserem Workshop: Alle vorgestellten Geräte sind im Seminarpreis enthalten und können anschließend mitgenommen werden. Dies ist ideal für den Aufbau eines eigenen "Red Team" im Unternehmen und bietet einen praktischen Mehrwert für alle Teilnehmer.

Unsere Schulungen sind praxis-erprobt und basieren auf den Erfahrungen aus zahlreichen Penetrationstests. Der Hak5 Pineapple „Evil WiFi“ Knoten, zum Beispiel, hat sich als besonders effektiv erwiesen, um Sicherheitslücken in Unternehmensumgebungen aufzudecken und das Bewusstsein für IT-Sicherheit zu schärfen.

SCHUTZMAßNAHMEN FÜR IHR UNTERNEHMEN

Natürlich wird im Workshop auch der Schutz gegen diese Geräte – der sogenannte "Blue Team" Schutz – unterrichtet. Damit sind Sie nicht nur in der Lage, potenzielle Angriffe zu erkennen und abzuwehren, sondern können auch effektive Sicherheitsstrategien entwickeln, um Ihr Unternehmen bestmöglich zu schützen.

Die Geräte werden zum Einkaufspreis in den Seminarpreis integriert, so dass das Seminar ohne gesonderte HW-Beschaffung auskommt

INTERESSE GEWECKT? JETZT ANMELDEN!

Lust auf Hardware-Hacks im Herbst? Melden Sie sich einfach bei uns, indem Sie auf diese Nachricht antworten oder mir eine direkte Nachricht schicken.

NEHMEN SIE GERNE KONTAKT ZU UNS AUF ÜBER INFO@LOG2.DE

Die geplanten Termine sind:

26. November 2024 bis 28.November2024

Ein möglicher Zusatztermin wäre der 3. Dezember 2024 bis 5. Dezember 2024.

Der Seminarpreis ist

3.400 EUR für drei Tage
plus 990 EUR Hardware-Kosten
ergibt einen Gesamtpreis von 4.390 EUR

Der Seminarort ist

IBS Schreiber Akademie Hamburg Zirkusweg

Hardware

Die Hardware wird vermittelt von HackmoD IT-Security & Pentest Tools