Bundestechnologiezentrum für
Elektro- und Informationstechnik

Buchungsnummer: **611492**

Seminar

Wireless Hacking

Kurzinfos

Zertifikat	Abschluss: Teilnahmebescheinigung
Kursplätze	12 Personen
Veranstaltungsort	Oldenburg
Unterrichtseinheiten	16 UE
Tagesform	Vollzeit

Termin: **28.06.2022-29.06.2022**
Uhrzeit: **1. Tag: 09.00 Uhr - 16.30 Uhr 2. Tag: 08.00 Uhr - 15.30 Uhr**

Kosten: **565 €**

Wireless-LAN bzw. WLAN ist nicht mehr wegzudenken. Die Einrichtung dieser Funk-Netze ist schnell geschehen und die Verbindungen sind nahezu überall verfügbar, um beispielsweise das Internet zu nutzen. Egal ob im Betrieb, zu Hause oder unterwegs in Hotspots, mit oder ohne Verschlüsselung, das WLAN ist allgegenwärtig.

Wie sicher sind jedoch diese WLAN-Verbindungen? Was wird verschlüsselt und wie? Ist der Datenstrom wirklich sicher? Welche Schwachstellen hat ein WLAN-Netz?

Mit diesem Training wird gezeigt, wie aktuelle WLAN nach dem Standard IEEE 802.11 funktionieren. In praktischen Übungen wird der Aufbau der Verbindungen gezeigt und beeinflusst. Der Zugriff und das Monitoring von WLAN-Access Points und den Datenströmen wird praktiziert. In Übungen werden die Schwachstellen von WEP und WPA Mechanismen erkannt. Mögliche Angriffsszenarien auf WLAN werden diskutiert und beispielhaft durchgeführt.

Alle praktischen Übungen erfolgen mit einer virtuellen Maschine und dem Hacking Tool Kali Linux. Für die Analyse der Datenströme kommt Wireshark zum Einsatz.

Eigene Laptops/Notebook können mitgebracht werden, wenn die Software darauf installiert werden kann und darf.

Inhalte

- Vorbereitungen der Umgebung
  - Installation/Konfiguration der virtuellen Maschine
  - Aktivierung der WLAN-Schnittstellen
- Suche und Identifikation von WLAN-AP
- WLAN Protocol Basics
  - Rahmenstruktur nach 802.11, Rahmentypen und Sub-Types
  - Einbettung in Ethernet
  - Methoden der Arbeitsweise
- Aufzeichnung von WLAN-Datenströmen
  - Analyse mit Wireshark
  - Selektion der Daten, Filterregeln in Wireshark
- Analyse der Access Points (APs)
  - Suche und Erkennung spezieller AP
  - Monitoring der Verbindungsaufnahme
  - grundlegende Beeinflussung von AP
- Verschlüsselung mit WEP
  - Methodik, Schwachstellen und Cracking von WEP
- Verschlüsselung mit WPA
  - Methodik und Schwachstellen
  - Cracking-Methoden von WPA
- Verbindungen mit verschlüsselten AP
  - Entschlüsselung der Datenströme
  - Verbindungsaufnahme an verschlüsselten AP
- Methoden der WLAN Angriffe
  - DoS Attacken
  - Störung eines Clients

Zielgruppen

Sie sind mit administrativen Aufgaben beim Kunden oder im eigenen Netz betraut und wollen Ihre Kenntnisse zu WLAN nach IEEE 802.11 vertiefen. Weiterführend wollen Sie Schwachstellen in Ihren WLAN-Konfigurationen finden und/oder durch Analyse des Betriebes optimieren.

Bei Beeinträchtigung des WLAN-Betriebes wollen Sie durch Monitoring mögliche Angriffe erkennen können.

bfe.de
Bundestechnologiezentrum für Elektro- und Informationstechnik e.V.
Donnerschweer Straße. 184, 26123 Oldenburg

Zielsetzung

Nach dem erfolgreichen Besuch sind Sie in der Lage Datenströme in einem WLAN aufzuzeichnen, zu analysieren und protokollarische Fehlerquellen zu erkennen. Mögliche Schwachstellen in der WLAN-Übertragung sind Ihnen bekannt. Sie kennen Nutzen und Schwachstellen von WEP und WPA /WPA2. Im Umgang üblicher Tools sind Sie vertraut und können eigene grundlegende Analysen im WLAN durchführen.

Voraussetzungen

Sie sind sicher im Umgang mit IP und kennen die grundlegenden WLAN Technologien. Bei der Analyse von Netzen haben Sie schon Wireshark kennen gelernt und sind mit der grundlegenden Bedienung vertraut.

Abschluss

Sie erhalten eine Teilnehmerbescheinigung mit detaillierter Angabe der Seminarinhalte.

Hinweis

Wireshark-Grundlagen werden in den BFE Seminaren „Fehlersuche im IP-Netz“ und „Fehlersuche bei VoIP und SIP“ vermittelt.

Unterkunft in Oldenburg

Unsere Angebote werden von Lernenden aus dem gesamten Bundesgebiet wahrgenommen. Das Bundestechnologiezentrum hat deshalb Sonderkonditionen mit ausgewählten Hotels der Stadt vereinbart.

Ansprechpartner

Michaela Tessendorf
T 0441 34092-133
m.tessendorf@bfe.de