The workshop ***"You're Watching - Tricks and Tools of Pentesters"*** provides a comprehensive technical understanding of a security check of IT systems - a so-called Penetration Test (Pentest).

The two-day workshop is aimed mainly at the IT staff of small and medium businesses who want to check or improve their IT security and get an understanding of how pentesting works. The workshop consists of practical and theoretical parts. The theoretical parts teach pentesting basics and give an introduction to different software tools.

The participants then use these tools to access a laboratory network and put the aquired knowledge into practice. We provide the necessary hardware and software. Each participant will receive a certificate of attendance and can take an optional exam to obtain a certificate of qualification.

Contact

Academic Management

Prof. Dr. Arno Wacker
Professor of Data Protection & Compliance

☎ 089 / 6004 - 7325
E-Mail: arno.wacker@unibw.de
Web: https://www.unibw.de/code

Forschungsinstitut Cyber Defence (CODE)
Universität der Bundeswehr München
Carl-Wery-Straße 22
81739 München

Support und Contact

Dipl.-Päd. Karina Anders, MBA
Coordination
campus advanced studies center

☎ 089 / 6004 - 2086
E-Mail: info@casc.de
Web: https://www.unibw.de/casc

campus advanced studies center
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85579 Neubiberg

Universität der Bundeswehr München

Workshop

You're Watching

Tricks and Tools of Pentesters

Forschungsinstitut Cyber Defence
Universität der Bundeswehr München

Workshop **You're Watching – Tricks and Tools of Pentesters**

Further information: https://www.unibw.de/casc/programme/zertifikate/pentest_en

The two-day workshop consists of six lessons and an optional exam. They are described in more detail below.

Lesson 1 – Introduction

This lesson explains the nature and structure of a penetration test and gives an overview of the pentesting tools used in the course of the workshop. Examples of tools are: Kali, Aircrack-ng, Nmap, Sqlmap and Metasploit.

Lesson 2 – Kali

First, the lecturers demonstrate how to start and navigate Kali. The participants then have the possibility to familiarize themselves with Kali and its tools using the provided laptops.

Lesson 3 – WLAN

The lesson begins with an explanation of the tool Aircrack-ng and of common weak points in a WLAN followed by a demonstration of Aircrack-ng in practice. After that the participants use Aircrack-ng to check the provided laboratory WLAN for security issues.

Lesson 4 – Scanning a network

This lesson is about collecting information in a network. It gives an introduction to the tool Nmap including the functionality for scanning a network and how to interpret the scan results. In the practical part the participants use Nmap to scan a laboratory network and interpret their findings.

Lesson 5 – Web security

This lesson has two topics from the field of web security, securing website content (SQL Injection) and secure transmission on the Web (HTTPS). It begins with an explanation of what an SQL injection is and a demonstration of the tool Sqlmap. A discussion on why HTTPS is important and a demonstration on how to check websites for their safety follows. Participants then use sqlmap to test a web portal for exploitable SQL injection vulnerabilities. The lesson concludes with testing website security using SSL Labs.

Lesson 6 – Metasploit

The lesson starts by showing where to get information on current vulnerabilities, followed by an overwiew of the metasploit framework and its functionality. After a demonstration of a network scan and exploit by example of EternalBlue, the participants use Metasploit to perform attacks in the laboratory network themselves.

Examination – Performing a pentest

Optionally, the participants can take part in an exam to receive a corresponding certificate of qualification. The exam takes place online within a timeframe of four weeks. For this purpose, the participants are provided with a VPN access to a network representing the IT of a small company in order to perform a pentest. To pass the exam, the participants need to go through all stages of an actual pentest, including contract preparation, finding at least 5 security vulnerabilities, and the preparation of a final report.