

Der Workshop ***You're Watching - Tricks und Tools der Pentester*** vermittelt ein umfassendes technisches Verständnis eines Sicherheitschecks der IT-Systeme - eines sogenannten *Penetration Tests (Pentest)*.

Der zweitägige Workshop richtet sich hauptsächlich an IT-Mitarbeiter von kleinen und mittelständischen Unternehmen, die die IT-Sicherheit in ihrem Unternehmen selbst überprüfen bzw. erhöhen möchten und/oder das Verständnis erlangen möchten, was ein Pentest für das eigene Unternehmen bedeutet. Er besteht aus praktischen sowie theoretischen Teilen. In den theoretischen Teilen werden zunächst jeweils die Grundlagen erläutert. Anschließend werden die konkreten Werkzeuge vorgestellt und vorgeführt, die in den praktischen Teilen eingesetzt werden.

Den Teilnehmern werden Laptops mit der benötigten Software bereitgestellt. Des Weiteren steht ein Labor-Netzwerk zur Verfügung. Dort kann (darf) das Gelernte direkt angewendet werden. Die Teilnehmer erhalten eine Teilnahmebescheinigung. Optional können die Teilnehmer später eine Prüfung durchführen und damit ein Zertifikat erhalten.

## Kontakt

### Inhaltliche Beratung

Prof. Dr. Arno Wacker  
Professor für Datenschutz und Compliance

☎ 089 / 6004 - 7325  
E-Mail: [arno.wacker@unibw.de](mailto:arno.wacker@unibw.de)  
Web: <https://www.unibw.de/code>

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

### Organisatorische Beratung

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

☎ 089 / 6004 - 2086  
E-Mail: [info@casc.de](mailto:info@casc.de)  
Web: <https://www.unibw.de/casc>

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



casc  
campus  
advanced  
studies  
center

## Workshop

# You're Watching

---

## Tricks und Tools

## der Pentester



**FI** Forschungsinstitut  
Cyber Defence  
Universität der Bundeswehr München

Der zweitägige Workshop besteht aus sechs Lerneinheiten und -optional- der Prüfung. Im Folgenden werden diese näher beschrieben.

### **Lerneinheit 1 – Einleitung**

In dieser Lerneinheit wird zunächst erklärt was ein Penetration-Test ist sowie sein systematischer Ablauf dargestellt. Anschließend wird eine Übersicht über Werkzeuge eines Pentesters gegeben, die im Laufe des Workshops von den Teilnehmern auch eingesetzt werden. Diese sind: Kali, Aircrack-ng, Nmap, Sqlmap und Metasploit.

### **Lerneinheit 2 – Kali**

Zunächst wird durch die Dozenten vorgeführt, wie man Kali startet und darin navigiert. Anschließend haben die Teilnehmer die Möglichkeit, sich auf den bereitgestellten Laptops mit Kali vertraut zu machen und über die in Kali mitgelieferten Tools einen Überblick zu verschaffen.

### **Lerneinheit 3 – WLAN**

Hier wird zunächst erklärt was das Werkzeug Aircrack-ng ist, welche Schwachstellen im WLAN es ausnutzt und welche Funktionen es umfasst. Anschließend wird vorgeführt, wie man Aircrack-ng in der Praxis einsetzt. Danach wenden die Teilnehmer selbst Aircrack-ng an, um das bereitgestellte Labor-WLAN auf Sicherheit zu überprüfen.

### **Lerneinheit 4 – Scannen eines Netzwerks**

In dieser Lerneinheit geht es um Sammeln von Informationen in einem Netzwerk. Die theoretischen Grundlagen dazu werden mit dem Vorstellen des Werkzeugs Nmap ergänzt. Hierbei wird erklärt welche Funktionen Nmap zum Scannen eines Netzwerks bietet und wie die Scan-Ergebnisse zu interpretieren sind. Im praktischen Teil wenden die Teilnehmer Nmap im Labor-Netzwerk selbst an und lernen die gesammelten Informationen zu deuten.

### **Lerneinheit 5 – Web-Sicherheit**

In dieser Lerneinheit werden manuelle sowie automatisierte Tests der Webseiten auf SQL-Injection-Anfälligkeiten behandelt. Hierbei wird zunächst erklärt, was eine SQL-Injection ist und warum sie funktioniert. Danach wird gezeigt, wie eine Web-Anwendung manuell auf SQL-Injection geprüft werden kann. Anschließend wird das Werkzeug Sqlmap vorgeführt, um die Überprüfung automatisiert durchzuführen. Im praktischen Teil werden die Teilnehmer Sqlmap in der Laborumgebung selbst einsetzen, um ein Webportal auf SQL-Injection-Schwachstellen zu prüfen und anzugreifen.

### **Lerneinheit 6 – Metasploit**

Zunächst wird erklärt, wo man Informationen über aktuelle Schwachstellen bekommt. Danach wird das Framework Metasploit vorgestellt und ein Überblick über seine Funktionen gegeben. Anschließend wird in dem Labor-Netzwerk die Suche nach Schwachstellen am Beispiel des EternalBlue-Exploits vorgeführt. Im praktischen Teil lernen die Teilnehmer Metasploit selbst anzuwenden und können das Labor-Netzwerk für ihre Angriffe nutzen.

### **Prüfung – Durchführung eines Pentests**

Optional können die Teilnehmer sich entscheiden eine Prüfung durchzuführen und dafür ein entsprechend gekennzeichnetes Zertifikat zu erhalten.

Die Prüfung findet online in einem Zeitraum von vier Wochen statt. Dafür wird den Teilnehmern ein VPN-Zugang zu einem weiteren Netzwerk zur Verfügung gestellt. Dieses Netzwerk bildet die IT eines kleinen Unternehmens nach und die Teilnehmer erhalten den Auftrag einen Pentest durchzuführen. Dabei müssen sie zum erfolgreichen Bestehen der Prüfung alle Schritte eines echten Pentests durchlaufen, d.h. insbesondere Vertragsausarbeitung, Finden von mindestens 5 Sicherheitslücken und das Erstellen eines Abschlussberichts.