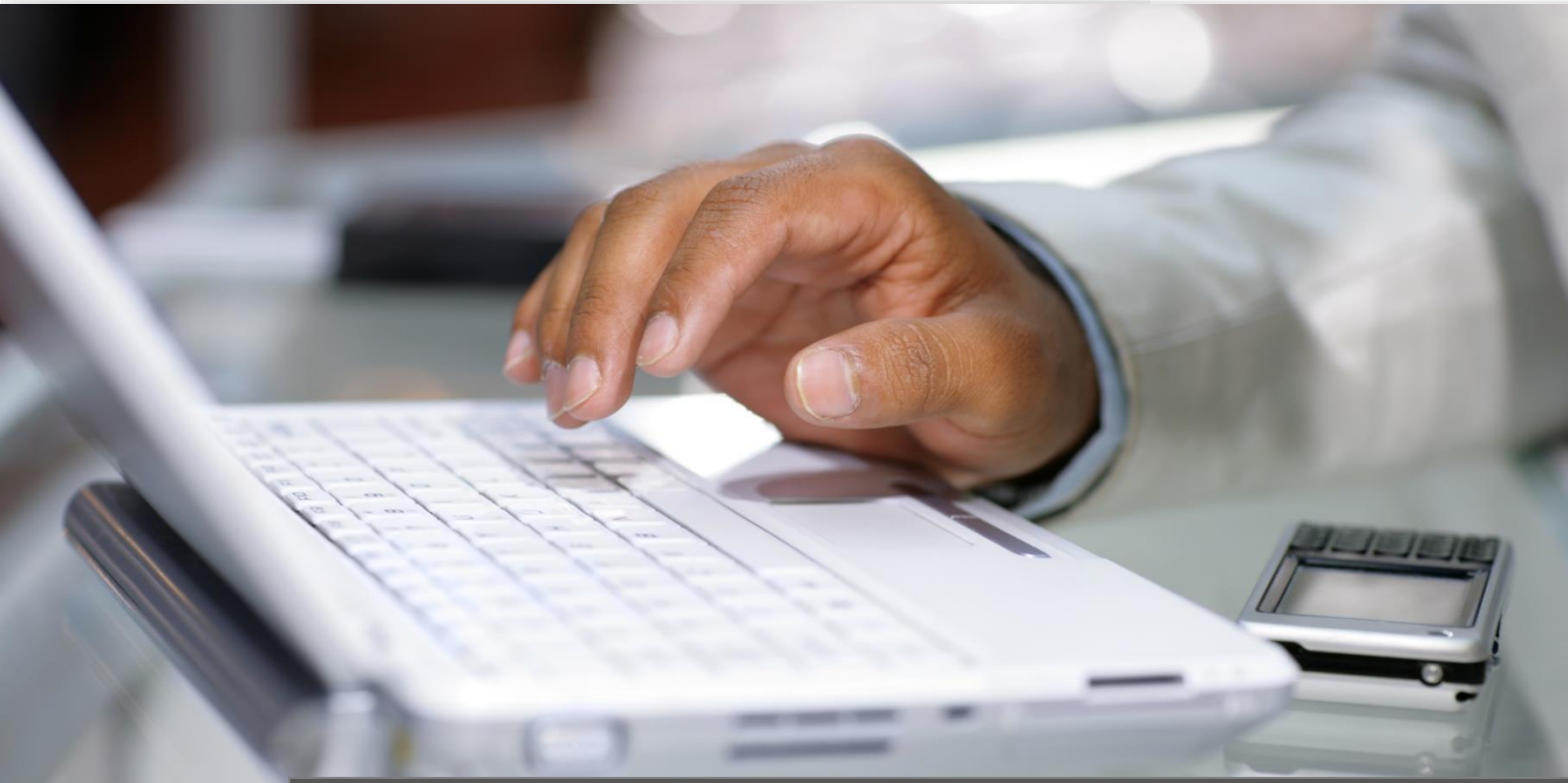
Certified Security Hacker

Online-Training | Examen CSH



Ausbildungsinhalte

ITKservice

Certified Security Hacker

Ausbildungspfad | Certified Security Hacker

Mit der Zertifizierung *Certified Security Hacker führen Sie in einem 24-stündigen Livehacking Examen den theoretischen und praktischen Nachweis* Sicherheitslücken von IT-Systemen erkennen und nutzen zu können.

	Online-Training	Dauer	Examen
	Certified Security Hacker	40 UE	CSH

Um sich wirksam vor Hacker-Angriffen zu schützen, muss man wissen, wie Hacker denken, wie sie vorgehen und welche Tools sie benutzen, um Schwachstellen zu erkennen - sprich man muss selbst zum Hacker werden, um sich optimal zu schützen. Genau dieses Wissen zu erlangen, steht im Fokus dieser sehr exklusiven Online-Ausbildungsreihe.
In dieser sehr praxisorientierten Online-Ausbildungsreihe erwerben Sie die notwendigen Kenntnisse, um als herstellerneutraler Sicherheitsexperte, IT-Systeme, Netzwerke und mobile Endgeräte in der Sicherheitskonfiguration auf Schwachstellen zu prüfen. Hierzu erlernen Sie das Scannen, Testen, und Schützen von ITK Systemen und sammeln viele praktische Erfahrungen.

	Unterrichtseinheit	UE 01	CSH

Einführung: Penetrationtesting & Hacking
- ✓ Wer sind die Angreifer?

Bedrohungspotential durch Hacker
- ✓ Script Kiddies
- ✓ Hacker
  - Individuum
  - Gruppe
  - Professionelle Hacker

Motivation der Angreifer
- ✓ Finanzielle Hintergründe
- ✓ Emotionale Hintergründe
- ✓ Idealistische Hintergründe
- ✓ Politische/Wirtschaftliche Hintergründe

Hacking im Wandel der Zeit
- ✓ 1960er – Ende 80er Jahre
- ✓ Jahr 1990+
- ✓ Jahr 2000+
- ✓ Jahr 2010+
- ✓ Bit & Bytes + Social Engineering
- ✓ Cyberwarfare + Real Warfare
- ✓ Cyberwarfare + Politik

Bedrohung für alle Unternehmen
- ✓ Ist Ihr Unternehmen in Gefahr?
- ✓ Effiziente Verteidigung

	Unterrichtseinheit	UE 02	CSH

Penetrationstesting – Methoden im Überblick
- ✓ Security Scan / Vulnerability

Vulnerability Scan
- ✓ Kommerzielle Scanner im Überblick
- ✓ Technische Hintergründe
- ✓ Vulnerability Database
- ✓ Vorteile
- ✓ Nachteile
- ✓ Gefahren

Penetrationstest
- ✓ Definition
- ✓ Vorgehensweise
- ✓ Vorteile
- ✓ Nachteile
- ✓ Gefahren

Sonderform: Ethical Hacker
- ✓ Emulation eines Hackerangriffs
- ✓ Vorteil
- ✓ Nachteil
- ✓ Gefahren

Der Richtige Weg
- ✓ Penetrationstest – korrekter Ablauf

Unterrichtseinheit	UE 03	CSH

KALI Linux - A Pentesters Friend
- ✓ Ursprung, Idee, Motivation hinter KALI
- ✓ Für Pentester und Hacker?

KALI Linux - Top Tools
- ✓ NMAP
- ✓ Maltego
- ✓ Vulnerability Database (Online)
- ✓ Vulnerability Scanner: OPenVAS

Echtes Penetrationstesting?

KALI Linux - Pentesting Setup

KALI Linux - Training Setup

Installationsanleitung KALI Linux

Installationsanleitung KALI Nethunter

Unterrichtseinheit	UE 04	CSH

Information Gathering
- ✓ Sun Tzu – The Art of War

Information im Cyberwarfare
- ✓ Information als 5ter Operationsraum

Information beim Hacking
- ✓ Art der Information
- ✓ Kennwörter Zugangsdaten
- ✓ Personen und Personengruppen
- ✓ Social Hacking (Engineering)
- ✓ Effekte des Social Hackings

Information beim Hacking
- ✓ FOCA Pro
- ✓ Metadaten
- ✓ Abwehr: Web Information Gathering
- ✓ Google Hacking
  - Information Gathering 2.0
  - Potentielle Risiken
  - Suchoperatoren
  - Advanced Suchoperatoren
  - Database

Unterrichtseinheit	UE 05	CSH

Information Gathering (Soziale Netzwerke)
- ✓ Kleinste Details & Informationen
- ✓ Private Soziale Netzwerke
- ✓ NSA für Jedermann
- ✓ Hacker Tools im Überblick

Information Gathering (Soziale Netzwerke)
- ✓ Fallbeispiel: Angriff auf Automobilkonzern
  - Wie könnte der Schaden aussehen?
  - Wie funktioniert so ein Angriff?
  - Wer hat den Schaden?

Unterrichtseinheit	UE 06	CSH

Information Gathering (Technisch)
- ✓ Technisches Information Gathering
  - Zielsetzung
  - Ziele identifizieren
- ✓ Domäne identifizieren
- ✓ Domäne Inhaber identifizieren
- ✓ Hostnamen in Domänen finden

Information Gathering (Technisch)
- ✓ Stärken der Methoden
- ✓ Analyse der gefunden Hostnames/IP-Adressen
- ✓ Werkzeuge

Unerkannt im Internet surfen
- ✓ Methoden, Anbieter und Tools

Unterrichtseinheit	UE 07	CSH

Scanning: Einführung
- ✓ Scanning
- ✓ Phase 1: Alive Detection
- ✓ ICMP Request / Ohne Reply
- ✓ ICMP / Wireshark – Raply Erfolgt
- ✓ ICMP Ping – Eingeschränkt brauchbar
- ✓ Alive Test mit NMAP

Scanning: Einführung
- ✓ TCP Connections – Kompaktform
- ✓ Jenseits des 3 Wege Handshake
- ✓ Warnhinweis: Grauzone Scanning endet
- ✓ Premission To Attack
- ✓ Scanning Übung

Unterrichtseinheit	UE 08	CSH

Scanning: Grundlagen und Tools
- ✓ Metasploitable als Zielscheibe
- ✓ Identifikation der Metasploitable IP-Adresse
- ✓ Verfügbarkeitstest unter KALI
- ✓ Nmap – Erste Schritte
- ✓ Nmap – Urscan

Scanning: Grundlagen und Tools
- ✓ Auswertung
- ✓ Ndiff
- ✓ Script Scans
- ✓ Nmap Timing Optionen
- ✓ Nmap für Hacker

Unterrichtseinheit	UE 09	CSH

Scanning: Grundlagen und Tools (Praktische Umsetzung)
- ✓ Metasploitable als Zielscheibe
- ✓ Identifikation der Metasploitable IP-Adresse
- ✓ Verfügbarkeitstest unter KALI
- ✓ Nmap – Fortsetzung
- ✓ Nmap – SYN Scan (-sS) mit Kompromissen
- ✓ Nmap – Weitere TCP Scan Methoden
- ✓ Nmap – UDP Scans

Scanning: Grundlagen und Tools (Praktische Umsetzung)
- ✓ Nmap – UDP Protokoll
- ✓ UDP Problem – Lösung
- ✓ Nmap Reports erstellen
- ✓ Nmap Reports anpassen
- ✓ Hping – Connectivity TesT
- ✓ Hping – TCP Connectivity Check
- ✓ Hping – weitere Funktionen

Unterrichtseinheit	UE 10	CSH

Scanning: Auswertung der Ergebnisse
- ✓ Metasploitable als Zielscheibe
- ✓ Identifikation der Metasploitable IP-Adresse
- ✓ Nmap -O- Identifikation des Zielbetriebssystems
- ✓ Nmap -A- All in One Methode

Scanning: Auswertung der Ergebnisse
- ✓ Evaluierungsscan für die Auswertung
- ✓ Exploit-DB.com
- ✓ CVEDetails.com

Unterrichtseinheit	UE 11	CSH

Vulnerability Scanning
- ✓ OpenVAS
  - Struktur und Aufbau
  - Überblick der Komponenten
  - Installation unter KALI Linux 2016.1
  - Konfiguration

Vulnerability Scanning
- ✓ OpenVAS
  - Erster Testlauf
  - Ergebnisse
  - Nessus Professional

Unterrichtseinheit	UE 12	CSH

Vulnerability Scanning
- ✓ OpenVAS
  - Erstellen eines Targets/mehrere Targets
  - Erstellen eines Target basierten Scans
  - Interne Systemüberprüfung
  - Zugangsdaten einrichten

Vulnerability Scanning
- ✓ Tasks mit Credentials erstellen
- ✓ Wiederholende Tasks erstellen
- ✓ Weitere Einblicke
- ✓ Nessus Scanning Configuration

Unterrichtseinheit	UE 13	CSH

Verifikation der entdeckten Schwachstellen
- ✓ Überprüfung der Schwachstellen
- ✓ Manuelle Suche nach Schwachstellen
- ✓ DISTCC: Proof of Concept & Shell Command Injection

Verifikation der entdeckten Schwachstellen
- ✓ Metasploit Framework
- ✓ Exploit mit Metasploit Framework ausführen
- ✓ Exploit mit Armitage ausführen
- ✓ Hail Mary! mit Armitage abfeuern

Unterrichtseinheit	UE 14	CSH

Auswertung der Ergebnisse
- ✓ CVSS im Vulnerability Scanning Bericht (OpenVAS)
- ✓ Erläuterung Common Vulnerability Scoring System
- ✓ CVSS 10.0 = Höchste Kritikalität
- ✓ CVSS Kritikalität der Samba Lücke
  - Samba Lücke unerkannt

Auswertung der Ergebnisse
- ✓ Ergebnisse von NMAP
- ✓ Kritikalität von indirekten Sicherheitslücken
- ✓ Prüfung der Zusammenhänge
- ✓ Kritikalität inhaltsbezogen
- ✓ Kritikalität von Webanwendung
- ✓ Kategorisierung von Schwachstellen

Unterrichtseinheit	UE 15	CSH

Erstellung eines Abschlussberichts
- ✓ Format eines Abschlussberichts, Deckblatt (Beispiel)
- ✓ Erläuterung „Scope“
- ✓ Auftragnehmer und Auftraggeber
- ✓ Definition des Scope – Zweiter Absatz
- ✓ Scope Verifikation
  - Interner Pentest
  - Externer Pentest
  - Weitere Optionen

Erstellung eines Abschlussberichts
- ✓ Testverfahren und Methoden
- ✓ Executive/Management Summary
- ✓ Schwachstellen
- ✓ Schwachstellendetails
- ✓ Proof of Concept Darstellung
- ✓ Auswirkung
- ✓ Handlungsempfehlung
- ✓ Zusammenfassung

Unterrichtseinheit	UE 16	CSH

Bedrohungsszenarien im Unternehmensnetzwerk
- ✓ Angriffe gegen das Unternehmen
- ✓ Lohnende Ziele
- ✓ E-Mail Communication Interception
- ✓ Bedrohung durch Malware
- ✓ Wirkung von Malware im Unternehmensnetz
- ✓ Erkennungsmethoden: Malware
- ✓ Malware Anomalien im LAN
- ✓ Malware Spuren per NSM finden
- ✓ Malware im Unternehmen: Immer bekämpfen!

Bedrohungsszenarien im Unternehmensnetzwerk
- ✓ Hacker im Unternehmensnetzwerk
- ✓ Detektion von Hackern
- ✓ Keylogger – Speziellangriff gegen Führungsspitze

Bonus Track: Pentesting Addons
- ✓ Bespiele für Spezialeinsätze
- ✓ Zertifikate eines Penetrationstester
- ✓ Spezialisierung bei Penetrationstest

Unterrichtseinheit	UE 17	CSH

Denial-of-Service Angriffe
- ✓ Typische Attacke für digital Erpresser (oder Aktivisten)
- ✓ Eine kurze Historie
- ✓ DoS Angriffe: Brandaktuell
- ✓ DoS Attack as a Service ...
- ✓ Was wird geboten?
- ✓ Live-Demo
- ✓ Welche Arten von DoS-Angriffen existieren?
- ✓ Einsatzgebiete für DoS-Angriffe
- ✓ DoS-Angriffe: Externe Bedrohung?
- ✓ Live Demo: Einfacher DoS-Angriff gegen eine Website

Denial-of-Service Angriffe
- ✓ Ergebnis: Apache: problemlos ausgeschaltet
- ✓ Gegenmaßnahmen: Webserver Überlastung
- ✓ Live Demo: Simulierter DDoS gegen Linux
- ✓ Ergebnis: Linux System bricht unter Load zusammen
- ✓ Gegenmaßnahmen: Flooding Attack
- ✓ Live Demo: OSI Layer 2 (ARP) Angriff
- ✓ Ergebnis: System nicht erreichbar, keine Effekte!
- ✓ Gegenmaßnahmen: ARPSpoof Angriff

Unterrichtseinheit	UE 18	CSH

Man-in-the-Middle Angriffe (inkl. VoIP)
- ✓ Abhör-und Manipulationsangriffstechnik
- ✓ Voraussetzung für MitM-Angriffe
- ✓ Szenario: Angreifer für Tethering Attacke durch KALI Nethunter
- ✓ Tethering Attacke im Detail
- ✓ Tethering Attacke: Angriffsziele
- ✓ Szenario: Angreifer nutzt (Rogue) Access Point
- ✓ Rogue Access Point - Live Demo

Man-in-the-Middle Angriffe (inkl. VoIP)
- ✓ Man-in-the-Middle Allround Tool: Ettercap
- ✓ Ettercap: Funktionsweise
- ✓ Ettercap Vorbereitungen für MitM - Live Demo
- ✓ ARP Spoofing Verifikation - Live Demo
- ✓ Ein klassisches Beispiel - Live Demo
- ✓ Ettercap - Weitere Optionen - Live Demo
- ✓ VoIP Angriffe mit Wireshark - Live Demo
- ✓ MitM: Angriffspotential?

Unterrichtseinheit	UE 19	CSH

Angriffe gegen SLS/TLS
- ✓ Kurze Einführung
- ✓ Secure Socket Layer (SSL)
- ✓ Transport Layer Security (TLS)
- ✓ SSL, TLS und Browser....
- ✓ SSL, TLS und offizielle Empfehlungen
- ✓ SSL, TLS vs Empfehlungen und Kompatibilität
- ✓ Verwirrung? Einfache Testmöglichkeit!
- ✓ Welche Angriffe existieren gegen SSL/TLS?
  - SSL Stripping
  - STARTTLS Command Injection
  - BEAST
  - Padding basierte Angriffe
- ✓ Welche Angriffe existieren gegen SSL/TLS?
  - CRIME
  - HEARTBLEED
  - DROWN
  - POODLE
  - S-O-R-G-L-O-S-I-G-Keit
  - Einfache Angriffstools in KALI Linux
  - Gestohlene / verlorene Root CA Zertifikate
- ✓ Wie sicher ist mein SSL/TLS - Server?
- ✓ Live Angriff mit SSL Strip!
- ✓ SSL/TLS: Angriffspotential?

Unterrichtseinheit	UE 20	CSH

WLAN Security & Hacking
- ✓ Wireless LAN (WLAN) – kurze Historie
- ✓ Sicherheitsprotokolle
  - Wired Equivalent Privacy (WEP)
  - Angriff gegen WEP mit Wifite - Live Demo
  - Wi-Fi Protected Access (WPA)
  - Cloud Cracker - Live Demo
  - Wi-Fi Protected Access 2 (WPA2)
  - WPA2/WPA Angriff mit Wifite - Live Demo
- ✓ Sonderstellung: WPS
  - Wi-Fi Protected Setup (WPS)
  - Pixie Dust Angriff gegen WPS Access Point – Live Demo

WLAN Security & Hacking
- ✓ Enterprise WPA/WPA2
  - Zusätzlicher Schutzlayer durch Radius Authentifikation
  - Kommerzielle Appliances von vielen Herstellern
  - WPA sollte *deaktiviert* werden
  - Reine Enterprise WPA2 Access Points nicht angreifbar
- ✓ Weitere Angriffe
  - Denial of Service Angriffe
  - Abhörangriffe
- ✓ Wireless LAN (WLAN)- KALI Tools
- ✓ WLAN Hacking Script

Unterrichtseinheit	UE 21	CSH

Brute Force und Dictionary Angriffe
- ✓ Definition
- ✓ Problematik
- ✓ Alternative: Brute Force/Dictionary Hybrid: CEWL
- ✓ Effizienz von Brute Force Listen
- ✓ CCUP: Common User Password Profiler
- ✓ John The Ripper
- ✓ Erfolgreiches Passwort Cracking

Brute Force und Dictionary Angriffe
- ✓ Hydra & Medusa: Angriffszweck in KALI
- ✓ Hydra im Überblick
- ✓ Medusa im Überblick
- ✓ Hydra & Medusa im Angriff gegen Metasploitable
- ✓ Hydra Special: Angriff auf Web basierten Login Seiten

Unterrichtseinheit	UE 22	CSH

Angriffe gegen Passwörter und Hashes
- ✓ Indirekte Passwort Attacken
- ✓ Kleines 1x 1: Windows Hashes
  - NTLMv2
  - Speicherung Hashes in Windows Password Dateien
  - Angriffsszenarien

Angriffe gegen Passwörter und Hashes
- ✓ Hackerangriff gegen Windowssystem
- ✓ Hashdump: Verschlüsselte Passwörter
- ✓ OPH Crack
- ✓ Side Attack: Physikalische Attacken
- ✓ KON-Boot: Angriff gegen Windows Server 2008 R2

Unterrichtseinheit	UE 23	CSH

Angriffe gegen Netzwerk Infrastruktur
(Angriff gegen die Domäne)
- ✓ David gegen Goliath
- ✓ Aufbau des Angriffs
- ✓ Angriff in der Praxis (Live Demo)
- ✓ Reiche(re) Beute: Im Arbeitsspeicher
- ✓ UAC Angriff: Benutzer Interaktion (Live Demo)
- ✓ Kein Speicherzugriff?
- ✓ Rein in den 64 Bit Prozess (Live Demo)

Angriffe gegen Netzwerk Infrastruktur
(Angriff gegen die Domäne)
- ✓ Hashdump funktioniert …
- ✓ Ab in den Memory…
- ✓ Kiwi / Mimikatz vs. Windows Domäne
- ✓ Domain Administrator Kennwort gehackt!
- ✓ Angriff gegen DC: Metasploit Methode
- ✓ Angriff gegen DC: SMBexec Methode

Unterrichtseinheit	UE 24	CSH

Angriffe gegen weitere Geräte
(Roundup: Pentest & Infrastruktur)
- ✓ Was ist übrig?
- ✓ Angriffe gegen Netzwerk Geräte
- ✓ Angriffe gegen Peripheriegeräte
- ✓ Risiko: Kopierstation
- ✓ Risiko: VLAN Segmente
  - Switch Spoofing
- ✓ Yersinia Framework – Angriffe im Netz

Angriffe gegen weitere Geräte
(Roundup: Pentest & Infrastruktur)
- ✓ Weitere Angriffsmethoden & Hacking Tools
  - 802.1X Angriffsmethode: Pwnie Express
  - Angriffsmethode: Keylogger
  - Angriffsmethode: Keylogger (Software)
  - Angriffsmethode: WiFi (Hacking Appliances)
  - Angriffsmethode: LAN Turtle
- ✓ Abschließendes

Unterrichtseinheit	UE 25	CSH

Web Security - Einführung
- ✓ Grundelemente des World Wide Web
- ✓ HyperText Markup Language (HTML)
- ✓ Uniform Resource Locator
- ✓ HyperText Transfer Protocol (HTTP)
  - Session-Management
  - REQUEST Methoden
  - Get Method im Überblick
  - Get Method mit Parameter
  - POST Methode mit Parameter
  - POST – GET Konvertierung

Web Security - Einführung
- ✓ Web Security & Hacking – allgegenwärtige Bedrohung
- ✓ Information at your fingertips
- ✓ Historie World Wide Web
- ✓ HTML Elemente – Sicherheitsfeature?
- ✓ Web Security Tool: Firefox
  - Web Developer
  - Firebug

Unterrichtseinheit	UE 26	CSH

OWASP Top 10 im Überblick
- ✓ Kurzvorstellung: Unsere Testzielscheibe
- ✓ Kurzvorstellung: OWASP Wiki Website
- ✓ Übersicht & Bedrohungsgrad
- ✓ A1 Injection
- ✓ A2 Broken Authentication & Session Management
- ✓ A3 Cross Site Scripting (XSS)
- ✓ A4 Insecure Direct Object References

OWASP Top 10 im Überblick
- ✓ A5 Security Misconfiguration
- ✓ A6 Sensitve Data Exposure
- ✓ A7 Missing Function
- ✓ A8 Cross Site Request Forgery (CSRF)
- ✓ A9 Using Components with Known Vulnerabilities
- ✓ A10 Unvalided Redirects and Forwards

Unterrichtseinheit	UE 27	CSH

OWASP A1 - Injections
- ✓ Kurzvorstellung: Unsere Testzielscheibe
- ✓ SQL Injections
- ✓ Erste Angriffsversuche (Firefox)
- ✓ Kleine Helfer: Firefox Addon „Hackbar“
- ✓ Bequemere Manipulationsmöglichkeiten mit Hackbar
- ✓ Mühselig trotz Hackbar?
- ✓ Session Management Problem

OWASP A1 - Injections
- ✓ SQLMap Angriff gegen DVWA
- ✓ Fortgeschrittene Angriffe mit SQLMap
  - Konfigurationsparameter auslesen
  - Datenbank, User, Passwort & Privilegien
  - Datenbankstruktur ausspionieren
- ✓ Manueller SQL Injection mit Strukturwissen
- ✓ SQL Injections abwehren

Unterrichtseinheit	UE 28	CSH

OWASP A2 – Broken Authentication
- ✓ Netsparker für Ihre eignen Anwendungen?
- ✓ Einführung A2 – Broken Authentication
- ✓ bWapp (Bee WAPP)
  - bWapp im Überblick - Live Demo
- ✓ bWapp Beispiel: Umgehen von CAPTCHA‘s
  - CAPTCHA Breaking mit Rumola - Live Demo
- ✓ Beispiele: Password Attacks & Weak Passwords
- ✓ Beispiele: Administrative Portals

OWASP A2 – Broken Authentication
- ✓ bWAPP Administrative Portals - Live Demo
- ✓ Beispiele: Cookies (HTTP-ONLY & Secure)
  - bWAPP Administrative Portals - Live Demo
- ✓ Beispiele: Session ID & Session Security
  - bWAPP Session ID’s und Strong Sessions - Live Demo
- ✓ OWASP A3 Cross Site Scripting

Unterrichtseinheit	UE 29	CSH

OWASP A3 – Cross Site Scripting
- ✓ Testzielscheibe
- ✓ Zweite Testzielscheibe: bWAPP
- ✓ Einführung
- ✓ Funktionsweise: Cross Site Scripting
- ✓ Ausnahme: Persistentes Cross Site Scripting
- ✓ Grundsätzliche Arten

OWASP A3 – Cross Site Scripting
- ✓ Einfache Beispiele mit DVWA und bWAPP
- ✓ Cross Site Scripting finden mit XSSer
- ✓ XSSer im Überblick
- ✓ Persistentes XSS
- ✓ XSS mit Schwachstellen

Unterrichtseinheit	UE 30	CSH

A4 – Insecure Object Direct Reference
- ✓ Testzielscheibe
- ✓ Zweite Testzielscheibe: bWAPP
- ✓ Einführung
- ✓ Weiteres Beispiel: Hidden Fields
- ✓ Neues Firefox Addon: Tamper Data
- ✓ Aufspüren A4… Keine leichte Aufgabe
- ✓ Weitere Web Security Tools in KALI Linux
  - BurpSuite
  - Commix
  - HTTrack

A4 – Insecure Object Direct Reference
- ✓ Weitere Web Security Tools in KALI Linux
  - OWASP Zap
  - Paros
  - Skipfish
  - SQLMap
  - W3AF
  - Webscarab
  - WPScan
  - JooScan

Unterrichtseinheit	UE 31	CSH

A5 – Security Misconfiguration
- ✓ Testzielscheibe
- ✓ Zweite Testzielscheibe: bWAPP
- ✓ Einführung
- ✓ Nikto – eine Alternative Scan Methode

A5 – Security Misconfiguration
- ✓ Nikto im Überblick
- ✓ Infrastruktur Security
- ✓ SNMP: Spionage des Zielsystems
- ✓ Weitere A5 Szenarien mit bWAPP

Unterrichtseinheit	UE 32	CSH

A6 – A10 – Schnellüberblick
- ✓ Testzielscheibe
- ✓ Zweite Testzielscheibe: bWAPP
- ✓ Einführung A6 – Sensitive Data Exposure
- ✓ Einführung A7 – Missing Function Level Access Control

A6 – A10 – Schnellüberblick
- ✓ Einführung A8 – Cross Site Request Forgery
- ✓ Einführung A9 – Using Components with Known Vulnerabilities
- ✓ Einführung A10 – Unvalided Redirect and Forwards

Unterrichtseinheit	UE 33	CSH

Automatisierte Web Scanner
- ✓ Testzielscheibe
- ✓ Zweite Testzielscheibe: bWAPP
- ✓ W3AF – KALI Linux
- ✓ OWASP ZAP

Automatisierte Web Scanner
- ✓ BURP Suite (Free & Pro)
- ✓ PAROS – KALI Linux
- ✓ WebScarab – KALI Linux
- ✓ Netsparker Pro (Commerziell)

Unterrichtseinheit	UE 34	CSH

Verifikation der Sicherheitslücken
- ✓ Testzielscheibe
- ✓ Zweite Testzielscheibe: bWAPP
- ✓ Scanning: Cross Site Scripting (A3)

Verifikation der Sicherheitslücken
- ✓ Scanning: Command Injection (A1)
- ✓ Scanning: SQL Injection (A1)
- ✓ Scanning: Security Misconfiguration (A5)

Unterrichtseinheit	UE 35	CSH

Bewertung der Sicherheitslücken
- ✓ Testzielscheibe
- ✓ Zweite Testzielscheibe: bWAPP
- ✓ Scanning: Cross Site Scripting (A3)

Bewertung der Sicherheitslücken
- ✓ Scanning: Command Injection (A1)
- ✓ Scanning: SQL Injection (A1)
- ✓ Scanning: Security Misconfiguration (A5)

Unterrichtseinheit	UE 36	CSH

Erstellung eines Abschlussberichtes
- ✓ Format eines Abschlussberichtes
- ✓ Deckblatt
- ✓ Erläuterung „Scope“
- ✓ Auftragnehmer und –geber
- ✓ Definition des Scopes
- ✓ Textverfahren und Methoden
- ✓ Executive/Management Summary

Erstellung eines Abschlussberichts
- ✓ Scope Verifikation
- ✓ Interner Test
- ✓ Externer Test
- ✓ Weitere Optionen
- ✓ Schwachstellen
- ✓ Kombinationen aufzeigen

Unterrichtseinheit	UE 37	CSH

Mobile Endgeräte - Einführung
- ✓ Mobile Computing
- ✓ Zwischenstufe: Tablet-Computer/PC
- ✓ Weiterentwicklung der Tablet Systeme
- ✓ Exotische Zwischenentwicklungsstufen
- ✓ Moderne Tablet Systeme
- ✓ Kurze Geschichte
  - Mobilfunknetzwerke in DE
  - Smartphone Entwicklung
- ✓ Moderne Smartphones
- ✓ Große Symbiose
- ✓ Historie: Android
  - Android Technologie im Überblick

Mobile Endgeräte – Einführung
- ✓ Historie: Apple
  - iOS 9 Highlights
  - iOS Technologie im Überblick
- ✓ Historie: Microsoft
  - Windows Phone Technologie
- ✓ App Stores
  - Apple App Store
  - Google Play Store
  - Amazon App Store
  - Microsoft Phone Store

Unterrichtseinheit	UE 38	CSH

Mobile Endgeräte – iOS Security
- ✓ Apple als Statussymbol
- ✓ Apple in der großen Politik
- ✓ Sicherheitskonzepte iOS
- ✓ Release: iOS Security Whitepaper
- ✓ Highlights iOS Security
- ✓ Secure Boot Chain
- ✓ DFU Modus
  - Howto
- ✓ System Software Authorization
- ✓ Secure Enclave
- ✓ Touch ID und Passwort
- ✓ Hardware Security Features

Mobile Endgeräte – iOS Security
- ✓ File Data Protection
- ✓ Passcodes
- ✓ Data Protection Classes
- ✓ Keychain Data Protection
- ✓ Keybags
- ✓ FIPS 140-2
- ✓ App Code Signing
- ✓ Runtime Process Security
- ✓ Data Protection in Apps
- ✓ iOS Jailbraek
- ✓ Angriffe gegen iOS

Unterrichtseinheit	UE 39	CSH

Mobile Endgeräte – Android Security
- ✓ Android im Vormarsch
- ✓ Sicherheitsfeatures ab Android 4
- ✓ Cold Boot Angriff gegen Android Systeme
- ✓ Android App Rechte
- ✓ Android Bootloader Schutz
- ✓ Empfehlung: Nexus Root Toolkit (NRT)
- ✓ Android Bootloader Unlock
- ✓ USB-Debugging Modus
- ✓ Sperroptionen

Mobile Endgeräte – Android Security
- ✓ Biometrie ausgetrickst
- ✓ Android Rooting
  - Samsung
  - Effekte
- ✓ Android Security Features
- ✓ Samsung Knox
- ✓ Mobile Forensik
- ✓ Zugriff auf Nutzdaten
- ✓ Zugriff auf mobile Endgeräte

Unterrichtseinheit	UE 40	CSH

Mobile Endgeräte – weitere Angriffe
- ✓ Mobilfunknetze
- ✓ GSM
- ✓ Protokoll
- ✓ Historie
- ✓ Problematik
- ✓ Unauthentifizierte Basisstation
- ✓ UMTS-Jammer: Downgrade auf GSM
- ✓ Rogue Basisstation
- ✓ GSM abhören
- ✓ USRP
- ✓ GNURadio
- ✓ Wireshark

Mobile Endgeräte – weitere Angriffe
- ✓ Kraken
- ✓ Rainbow Tables gegen A5/1-Verschlüsselung

Angriffe gegen WLAN/Mobile Hotspot
- ✓ Angriffe über Mikrofon und Kamera
- ✓ QR-Codes
- ✓ Was ist das?
- ✓ Gefahrenpotential
- ✓ Angriffe über das Mikrofon
- ✓ Viren und Malware bei mobilen Geräten
- ✓ Gefälschte SMS-Nachrichten
- ✓ iCloud Backup Stealing

Weitere wichtige Informationen

Ihr Trainer: Herr Thomas Wittmann

Der Trainer dieser exklusiven Online-Ausbildungsreihe ist Herr Thomas Wittmann. Er ist ca. 20 Jahren im Bereich IT-Security aktiv. Er ist einer der erfahrensten Sicherheitsexperten Deutschlands!

Neben einer umfangreichen Praxiserfahrung trägt er unter anderem die Titel *Professional Security Analyst Accredited Certification (OPSA)*, *Professional Security Tester Accredited Certification (OPST)* und *Offensive Security Certified Professional (OSCP)*. Zudem ist er als Oracle Datenbank-Spezialist, System-administrator und Datenschutzbeauftragter aktiv. Hierüber hinaus verfügt er über sehr viel Erfahrung als national und international tätiger Penetrationstester und dies auch in hochkritischen Bereichen wie beispielsweise regierungsnahen Umgebungen.

Als „Ex-Hacker" gibt er immer wieder Interviews zum Thema IT-Sicherheit und wird auch gerne als TV-Experte zu Rate gezogen (vor kurzem wieder im WDR, wo er den Zuschauern die Problematik eines Hackerangriffes auf SmartHome-Systeme der Telekom aufzeigte).

Optimale Prüfungsvorbereitung

Etwa drei Tage vor der Prüfung zum *Certified Security Hacker* erhalten Sie alle notwendigen Prüfungsunterlagen und eine detaillierte Anleitung, wie Sie die Prüfung ablegen können und was das Ziel Ihres Angriffs ist.

Tipp: Werfen Sie zudem einen Blick auf die Kapitel 7 bis 12 und 21 (mit Fokus auf das dort beschriebene CUPP).

Sie haben Fragen oder Anregungen?

Falls Sie Fragen, Wünsche oder Anregungen zu dieser oder zu anderen Ausbildungen haben, stehen wir Ihnen montags bis donnerstags in der Zeit von 08:00 – 17:00 Uhr und freitags von 08:00 – 13:00 Uhr sehr gerne zur Verfügung.

Sie erreichen uns unter:

Telefon: 09526 95 000 60
E-Mail: info@ITKservice.NET

Ihre Ansprechpartner für das ITKwebcollege.Security Hacker

Christoph Holzheid
Anne Hirschlein
Sylvia Sonntag
Thomas Wölfel

Copyrights und Vertragsbedingungen

Kontaktdaten | Impressum

ITKservice GmbH & Co. KG
Fuchsstädter Weg 2
97491 Aidhausen

Telefon: 09526 95 000 60
Telefax: 09526 95 000 63

www: ITKservice.NET
E-Mail: info@ITKservice.NET

Sitz der Gesellschaft: Aidhausen | Amtsgericht Bamberg, HRA 11009, Ust-Id: DE 262 344 410 | Vertreten durch: Thomas Wölfel (GF).

Bildnachweise: Alle in diesem Dokument dargestellten Bilder wurden von der ITKservice GmbH & Co. KG bei ccvision.de lizensiert.
Redaktion: ITKservice GmbH & Co. KG | Copyright © 2018 ITKservice GmbH & Co. KG.