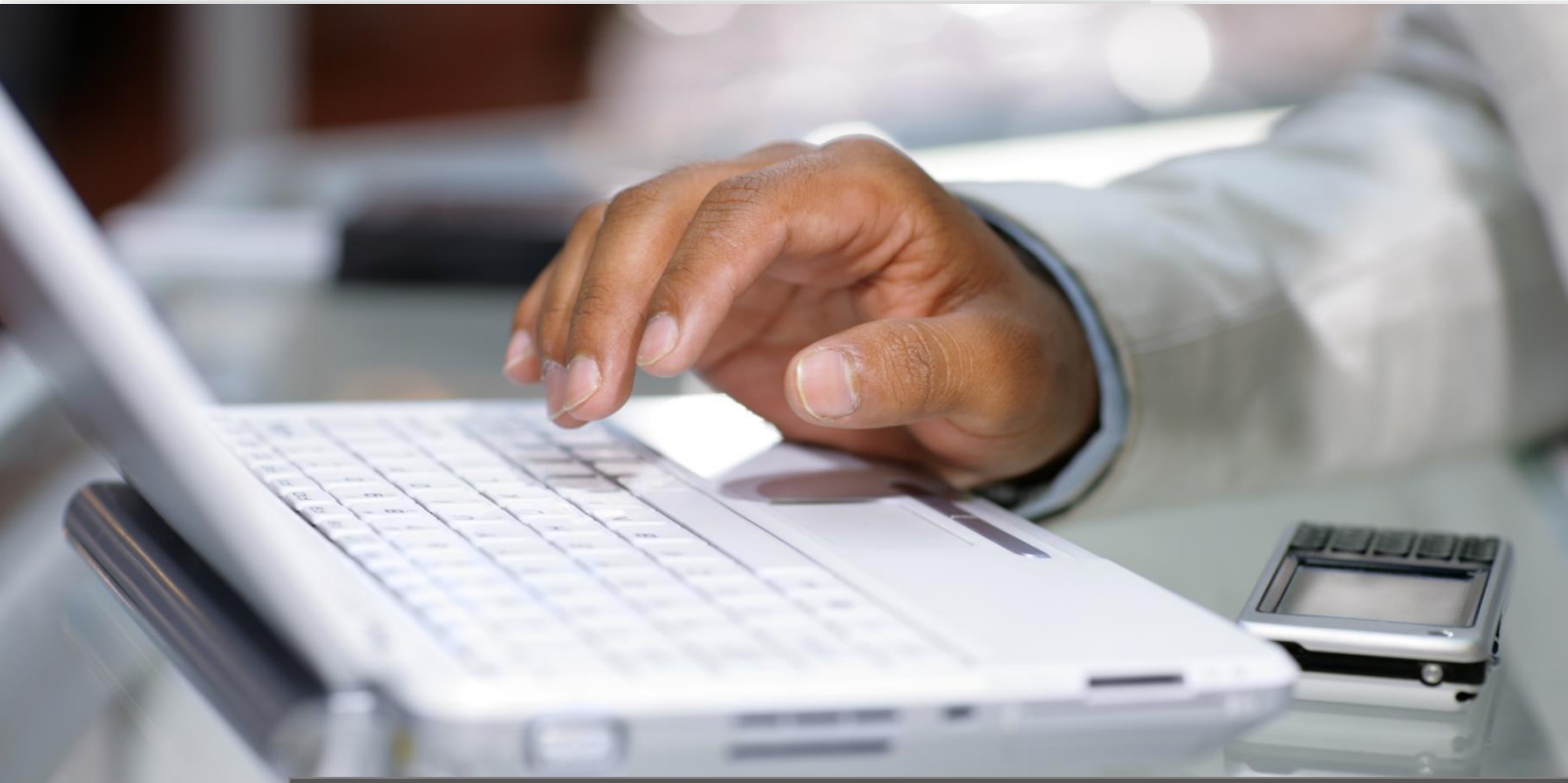
Certified Security Hacker 2020

Online-Training | Examen CSH 2020



Ausbildungsinhalte

ITKservice

Certified Security Hacker 2020

Ausbildungspfad | Certified Security Hacker 2020

CSH

CSH 2020
Certified Security Hacker 2020

Mit der Zertifizierung *Certified Security Hacker 2020 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

Hacking im Wandel der Zeit
- ✓ Zeitraum: 1960 – 1980er, 1990+, 2000+, 2010+, 2015+, Heute
- ✓ Cyberwarfare + Real Warfare

Hacker vs. Penetrationstester
- ✓ Hacking vs. Penetrationstesting
- ✓ Wer sind die Angreifer?
- ✓ Script Kiddies
- ✓ Hacker
  - Einzelperson
  - Gruppen
  - Professionelle
- ✓ Finanzielle Hintergründe
- ✓ Emotionale Hintergründe
- ✓ Idealistische Hintergründe
- ✓ Wirtschaftliche und Politische Gründe

Penetrationstesting
- ✓ Was ist ein Penetrationstest?
- ✓ Automatisiert?
- ✓ Manuell – Menschlich?
- ✓ Vorteile
- ✓ Nachteile
- ✓ Gefahren
- ✓ Der richtige Weg

	Unterrichtseinheit	UE 02	CSH

KALI Linux & Zielscheiben Einrichtung
- ✓ Testlabor – Umgebung für Pentester
- ✓ Hardware Anforderungen
- ✓ KALI Linux Installationsvorbereitungen
- ✓ KALI Linux Konfigurationsvorbereitungen
- ✓ Zielscheiben für dieses Training
- ✓ Vagrant: Virtuelle Images automatisieren
- ✓ Vagrant Box: win2k8 (metasploitable)
- ✓ Vagrant Setup für Windows
- ✓ Vagrant Setup für Ubuntu
- ✓ Start der beiden Vagrant Boxen
- ✓ KALI Linux Schnelltest

Unterrichtseinheit	UE 03	CSH

Funktionscheck der Ziele & KALI 2020.01
- ✓ Funktioniert das Testlabor
- ✓ Lösungen
- ✓ Vollständiger Funktionstest
- ✓ Syntex im Detail
- ✓ Ping funktioniert nicht
- ✓ KALI Linux
  - Besonderheiten
- ✓ KALI Linux 2020.1 Neuerungen

Unterrichtseinheit	UE 04	CSH

Information Gathering (Teil 1)
- ✓ Letzte Worte zum Laborsetup
- ✓ Sun Tzu – The Art of War
- ✓ Information als fünfter Operationsraum
- ✓ Auf welche Informationen kommt es an?
- ✓ Kennwörter und Zugangsdaten
- ✓ Social Engineering (Social Hacking)
- ✓ Art der Informationen
- ✓ FOCA – mächtige Waffe für Hacker
- ✓ FOCA gegen Berlin – Ergebnisse
- ✓ Erläuterung: Metadaten
- ✓ Verteidigungsmaßnahmen
- ✓ Google Hacking
  - Verbesserte Info.Gathering
  - Potentielle Risiken
  - Suchoperatoren
  - Der fehlende Syntax

Unterrichtseinheit	UE 05	CSH

Information Gathering (Teil 2)
- ✓ Der Teufel liegt im Details
- ✓ Stadt Berlin – die Zweite
- ✓ Berlin auf Xing und LinkdIn
- ✓ Berlin mit Hacker Tools betrachtet
- ✓ Was würde ein Hacker tun?
- ✓ OSINT
  - Was ist das?
  - Ziele von OSINT Operationen
  - Informationsquellen
  - Kurze Historie
  - Wie macht man OSINT?
  - OSINT mit KALI 2020.1 Linux

Unterrichtseinheit	UE 06	CSH

Information Gathering (Teil 3)
- ✓ Technisches Information Gathering
- ✓ Stärken der Methoden
- ✓ Web-Sites für DNS-Analysen
- ✓ IP- und DNS-Information
- ✓ Analyse der gefunden Hostnames
- ✓ Scrapebox

Unterrichteinheit	UE 07	CSH

Scanning (Teil 1)
- ✓ Hochfahren des Testlabors
- ✓ NMAP – der Scanner
- ✓ TCP/IP – Basisinformationen
- ✓ Scanning – Aufgaben
- ✓ Phase 1: Geräte per Scan erkennen
- ✓ Geräte im LAN Segment erkennen
- ✓ Phase 2: Erkennung von Systemdiensten
- ✓ 1000 – 65535 – oder Top 100?
- ✓ Szenarien und Beispiele
- ✓ Zeitprobleme beim Pentesting
- ✓ Phase 3: Parameter für OS Erkennung
- ✓ Phase 3: Parameter für Service Erkennung
- ✓ Script Scans per NMAP

Unterrichteinheit	UE 08	CSH

Scanning (Teil 2)
- ✓ Vulnerability Scanning
- ✓ NSE Scripts
- ✓ Weitere NMAP Optionen im Überblick
- ✓ Manuelle Schwachstellen Identifikation
- ✓ Manuelle Überprüfung in der Praxis
- ✓ OpenVAS
  - Übersicht
  - Installation
- ✓ Nessus
  - Überblick
  - Installation
- ✓ Metasploit Framework – Erste Schritte

Unterrichteinheit	UE 09	CSH

Vulnerability Scanning
- ✓ Ergebnisse der Schwachstellenscans
- ✓ Beispiel 1: FTP auf Ubuntu 14.04
- ✓ Welche Form von Exploit war das?
- ✓ Suche nach Local Privilege Escalation
- ✓ Beispiel 2: MS15-034
  - Schwachstellen IIS
  - Metasploit

Unterrichteinheit	UE 10	CSH

Pentest Box – für effizientes
- ✓ Gut sortierter Werkzeugkasten
- ✓ 100% gibt es nicht
- ✓ Optimiert aus Erfahrung
- ✓ Thema: Laptop(s)
- ✓ Lösung zum Laptop Dilemma: APU4
- ✓ Vorzüge eines APU4 Boards
- ✓ Reicht die CPU und das RAM?
- ✓ Was steckt in meiner APU?
- ✓ APU4
  - Installation
  - Baukasten
- ✓ Ubuntu per VMware Workstation installieren
- ✓ Für Serielle Konsolen anpassen
- ✓ FREE ESXi
- ✓ Szenarien und Installation
- ✓ OpenVAS 9 für Ubuntu 18.04
- ✓ Nessus für Ubuntu 18.04
- ✓ NMap für Ubuntu 18.04

Unterrichteinheit	UE 11	CSH

Vulnerability Scanning – Detailergebnisse
- ✓ Wie gehen wir im Detail vor?
- ✓ Erweiterung der Nessus Scans
- ✓ Schwachstelle: Windows SMB (2008R2)
- ✓ Exploit: Windows SMB (2008R2)
- ✓ Zwischenstation: Hashdump
- ✓ ManageEngine Angriff
- ✓ Weitere Remote Exploits?

Unterrichteinheit	UE 12	CSH

Weitere Vulnerability Scans & Methoden
- ✓ Verwundbarkeiten, IT und Menschlichkeit
- ✓ Szenario 1: Third Party Anwendungen
- ✓ Horror Szenario 1: Online Banking
- ✓ Wie löst man dieses Problem?
- ✓ Kostenloses Tool. Network Scanner
- ✓ Szenario 2: Dateien in Windows Shares
- ✓ Horror Szenario 2: Des Teufels Shares
- ✓ Lösung für des Teufels Shares!
- ✓ Added Value: Anerkennung
- ✓ Apropos Datenschtuz
- ✓ PtA – Komplex
- ✓ Weitere Sonderfälle
- ✓ IT Security bei Sonderanwendungen

Unterrichteinheit	UE 13	CSH

Local Privilege Escalation Exploits
- ✓ Zielsystem zusammen gehackt
- ✓ Suche nach den LPEs
- ✓ Local Privilege Escalation gegen Linux
- ✓ Local Privilege Escalation gegen Windows
- ✓ Remote Acces Toolkit (RAT)
- ✓ Erkennung von RATs
- ✓ Häufig im Einsatz: Trickbot
- ✓ RATs im Internet finden
- ✓ Überleitung zum Domain Hacking

Unterrichteinheit	UE 14	CSH

Windows Domain Hacking (I)
- ✓ Grenzgebiet
- ✓ Kleines Testlabor
- ✓ Vagrant/Packer
- ✓ Image von Windows 7 – 2019
- ✓ Packer Windows (Templates) im Überblick
- ✓ Bau eines VirtualBox Image
- ✓ Bausteine für unser DC Hacking Lab
- ✓ Zeitaufwand für den Bau
- ✓ Build Boxes zu Vagrant hinzufügen
- ✓ Informationen zum Vagrant File
- ✓ AD Hacking Tool: Empire Framework 3.1
- ✓ Hilfestellungen zu Vagrant

Unterrichtseinheit	UE 15	CSH

Windows Domain Hacking (II)
- ✓ Aufbau einer Testdomain
- ✓ DC einrichten
- ✓ Genug des AD Setups
- ✓ Empire Framework
  - Listeners
  - Launcher Payloads
- ✓ Payloads, Pentests und Antiviren
- ✓ Erste Schritte im gehackten System
- ✓ Vorgehen bei Empire
- ✓ Übernahme von Prozessen

Unterrichtseinheit	UE 16	CSH

Windows Domain Hacking (III)
- ✓ Windows AD Hacking und OSI Layer 8
- ✓ Szenario 1: AD User = Local Administrator
- ✓ Szenario 2: Benutzer erhält Sonderrechte
- ✓ Szenario 3: Services vorschnell installiert
- ✓ Der Mix machts
- ✓ Wenn die letzte Bastion fällt
- ✓ Und wenn das AD sauber ist?

Unterrichtseinheit	UE 17	CSH

Windows Domain Hacking (IV)
- ✓ Hidden Track: Übernahme ohne Zugang
- ✓ Konfiguration der Pentesting Box
- ✓ Sinn: Pentesting Box
- ✓ Change auf Erfolg dieses Angriffs
- ✓ Weitere Fakts zum AD Hacking
- ✓ PingCastle (für Windows)
- ✓ DarkSide: CrackMapExec

Unterrichtseinheit	UE 18	CSH

Network Security Monitoring (I)
- ✓ Historie
- ✓ Security Onion: NSM Systems
- ✓ Grundfunktionen/Tools
- ✓ Einsatzgebiete
- ✓ Aufgaben der Security Onion
- ✓ Testalarm für Security Onion
- ✓ NSM Konsole im Überblick
- ✓ Live System im Überblick
- ✓ Dienstleistungen NSM

Unterrichtseinheit	UE 19	CSH

Network Security Monitoring (II)
- ✓ Testaufbau
- ✓ Einsatzbeispiel
  - Scanning
  - Vulnerability Scanning
  - Exploitation
  - AD Hacking

Unterrichtseinheit	UE 20	CSH

Network Security Monitoring (III)

- ✓ NSM im Rahmen von Pentests
- ✓ IDS Sensorik auf Pentest Box installieren
- ✓ IDS Sensor: Suricata installieren
- ✓ Suricata 5.0
- ✓ Ruleset für Suricata holen
- ✓ Suricata starten/Autostart
- ✓ Logs nach ELK und Co
- ✓ Empfänger für Filebeat 7 – ELK Stack bauen
- ✓ Filebeat für ElasticCloud anpassen
- ✓ ElasticCloud im Überblick
- ✓ Weitere Ausbaustufen für „Mein Sensor“

Unterrichtseinheit	UE 21	CSH

Pentest: Bewertung der Ergebnisse

- ✓ Reichlich Ergebnisse
- ✓ NMAP
  - Ergebnisse
  - Beispiel
- ✓ Apache 2.2.21 Detailanalyse
- ✓ Bedeutung der CVE Werte
- ✓ Erläuterung Common Vulnerability Scoring System
- ✓ CVSS in Vulnerability Scans enthalten
- ✓ Wann meldet man eine Schwachstelle
- ✓ Praktische Umsetzung: manuell Methode
- ✓ Magische Werkzeug: NamicSoft
- ✓ Kritikalität vs. Kritische Inhalte
- ✓ Ergebnisse Domäne Hacking
- ✓ Totale Durchschüsse/DomAdmin Hacks

Unterrichtseinheit	UE 22	CSH

Pentest: Erstellung eines Abschlussberichts

- ✓ Format des Abschlussberichts
- ✓ Erster Abschnitt
  - Deckblatt
  - Erläuterung „Scope“
  - Beispiel Deckblatt
  - Auftraggeber & Auftragnehmer
  - Einführung/Beschreibung
  - Definition des Scope – Zweiter Absatz
  - Testverfahren und Methoden
  - Executive/Management Summary
- ✓ Zweiter Abschnitt
  - Scope Verifikation
  - Interner Pentest
  - Externer Pentest
  - Weitere Optionen
- ✓ Dritter Abschnitt
  - Schwachstellen
  - Schwachstellendetails
  - Proof of Concept
  - Auswirkung
  - Handlungsempfehlungen
- ✓ Vierter Abschnitt: Zusammenfassung

Unterrichtseinheit	UE 23	CSH

Angriffe gegen Passwörter und Hashes
- ✓ Quellen der Passwörter
- ✓ Voraussetzung der Extraktion
- ✓ Brute Force Angriffe – sinnvoll?
- ✓ Dictionary Attacks – sinnvoll?
- ✓ Was ist dann sinnvoll?
- ✓ Common User Passwords Profiler
- ✓ John the Ripper
- ✓ Direkte Angriffsmethoden gegen Hashes

Unterrichtseinheit	UE 24	CSH

Bedrohungen für das Unternehmen
- ✓ Was ist eigentlich realistisch
- ✓ Wie sieht so eine Veröffentlichung aus
- ✓ Hacken für Geld mit Ransomware
- ✓ Eintrittskanäle für Hacken mit Ransomware
- ✓ Der Testarbeitsplatz
- ✓ 0-Days können wir wohl ausschließen

Unterrichtseinheit	UE 25	CSH

Firewall Pentesting
- ✓ Thema Firewall
- ✓ Wie führt man Firewall Tests effizient durch
- ✓ Ziel IP-Adressen aufbauen
- ✓ Digital Ocean Droplet erstellen
- ✓ Zugriff und Konfiguration auf das Droplet
- ✓ Externe IP des Kunden (Pentest) ermittlen
- ✓ TCPDump vorbereiten
- ✓ Feuer auf das Ziel: per NMAP
- ✓ TCP Breakthrough Test
- ✓ UDP Breakthrough Test
- ✓ Auslesen der Ergebnisse
- ✓ Auswertung per Shell Skripting
- ✓ Pentest Bericht
- ✓ Rolle der Pentestbox

Unterrichtseinheit	UE 26	CSH

Firewall Pentesting - Spezialprotokolle
- ✓ Thema Firewall – Mission Impossible
- ✓ Digital Ocean Droplet erstellen
- ✓ Erweiterungen unseres Droplots
- ✓ Prüfung per TOR
- ✓ Abwehr von TOR
- ✓ Iodine – DNS Tunnel der Oberklasse
- ✓ Installation
- ✓ Ausführung der Prüfung
- ✓ Hans – Tunnelaufbau per ICMP
- ✓ Installation
- ✓ Ausführung der Prüfung
- ✓ Weitere Tunnel/Methoden

Unterrichtseinheit	UE 27	CSH

Web Security – Einführung
- ✓ Web Security – Das Buch mit 7(+) Siegeln
- ✓ Historie zum World Wide Web
- ✓ Grundelemente des WWW
- ✓ Hyper Text Markup Language (HTML)
- ✓ Uniform Resource Locator (URL)
- ✓ Hyper Text Transfer Protocol (HTTP)
  - Session Management
  - Request Methoden
  - Sichere und unsichere Methoden
  - GET Methode im Überblick
  - GET Methode mit Parametern
  - POST Methode mit Parametern
  - POST Konvertierung
- ✓ HTML Elemente als Sicherheitsfeature
- ✓ Web Security Tool der Profis: Firefox
- ✓ Firefox: Die besten Addons

Unterrichtseinheit	UE 28	CSH

Bedrohungen für das Unternehmen
- ✓ Was ist eigentlich realistisch
- ✓ Wie sieht so eine Veröffentlichung aus
- ✓ Hacken für Geld mit Ransomware
- ✓ Eintrittskanäle für Hacken mit Ransomware
- ✓ Der Testarbeitsplatz
- ✓ 0-Days können wir wohl ausschließen

Unterrichtseinheit	UE 29	CSH

Web Security: OWASP A1 im Dojo
- ✓ Web Security Dojo: Überblick
- ✓ Testzielscheibe im Dojo: DVWA
- ✓ SQL Injections mit Dojo/DVWA
- ✓ Unterstützung durch Debugging Funktionen
- ✓ SQL Injections automatisiert
- ✓ SQLMap scheitert an der Login Maske
- ✓ SQLMap unterstützt Cookies
- ✓ SQLMap speichert Ergebnisse
- ✓ SQLMap
  - Fortgeschrittene Funktionen
  - Der große Datendieb
- ✓ SQLMap in Deep

Unterrichtseinheit	UE 30	CSH

Web Security: OWASP A1 & A7
- ✓ Web Security Dojo: Überblick
- ✓ Testzielscheibe im Dojo: DVWA
- ✓ Command Injection mit Dojo/DVWA
- ✓ Manuelle Analyse der OS Injection
- ✓ Weitere Web Schwachstellenscanner
- ✓ Kommerzieller Scanner: Netsparker
- ✓ Cross Site Scripting (XSS)
- ✓ Gefahren von XXS
- ✓ XXS – OpenBugBounty Projekt

Unterrichtseinheit	UE 31	CSH

Web Security: OWASP A7 (XSS)
- ✓ Web Security Dojo: Überblick
- ✓ Testzielscheibe im Dojo: DVWA
- ✓ Cross Site Scripting (XXS) Allgemeines
- ✓ Gefahren von XXS
- ✓ Sonderfall: Stored Cross Site Scripting
- ✓ Gefahren von Stored XXS
- ✓ Drive by Download – Malware per Exploit Kit
- ✓ Exploit Kits (EK) – Überblick
- ✓ Cross Site Request Forgery (XSRF)
- ✓ Cross Site Scripting im Dojo
- ✓ XXS – OpenBugBounty Projekt

Unterrichtseinheit	UE 32	CSH

Web Security: OWASP Weitere Kategorien
- ✓ Web Security Dojo: Überblick
- ✓ Testzielscheibe im Dojo: DVWA
- ✓ A6 – Security Misconfiguration
- ✓ A3 – Sensitive Data Exposure
- ✓ A9 – Using Components with Known Vulnerabilities
- ✓ Weitere A-Kategorien
- ✓ Web-Security-Reports

Unterrichtseinheit	UE 33	CSH

Web Security: OWASP A10 und Absicherung
- ✓ Logging und Monitoring
- ✓ Einfaches Beispiel: SQL Injections
- ✓ Einfache Indikation: Logeinträge im Acces Log
- ✓ Komplexer Aufbau: Logs an ELK Server senden
- ✓ Alternative, lokale Web Analyse Tools
- ✓ Monitoring Systeme
- ✓ Logfile & Monitor, was noch
- ✓ Abwehr für Spezialanwendung

Unterrichtseinheit	UE 34	CSH

The Dark Side: Hacker im TOR-Netzwerk
- ✓ Entstehungsgeschichte
- ✓ Militärischer Einsatz des TOR-Netzwerks
- ✓ Weitere Möglichkeiten des Angriffs
- ✓ Wie funktioniert das TOR-Netzwerk
- ✓ TOR Verbindungsaufbau
- ✓ TOR Datenübertragung
- ✓ Facts
- ✓ TOR-Exit-Nodes
- ✓ Tiefe der TOR Kommunikation
- ✓ TOR-Kommunikation: Mögliche Ziele
- ✓ TOR effektiv nutzen
- ✓ KALI hinter Whonix Gateway
- ✓ Nachtrag: Proxychains für TOR nutzen

Unterrichtseinheit	UE 35	CSH

The Dark Side: Hacker im TOR-Netzwerk II
- ✓ Qubes OS im Überblick
- ✓ Spezielle Qubes Hardware
- ✓ Whonix bereits fest integriert
- ✓ TOR Hidden Services
- ✓ TOR Hidden Services + SSH = ?
- ✓ TOR-SSH-Tunnel im Überblick
- ✓ Windows als Pentest/Hacking Maschine

Unterrichteinheit	UE 36	CSH

WLAN & NAC Hacking
- ✓ WLAN Hacking – Stark überbewertet!
- ✓ Klassisches WLAN Hacking mit aircrack-ng
- ✓ Aircrack-NG vs. WPA/WPA2
- ✓ Aircrack-NG vs. WEP
- ✓ Simple WLAN Hacking Tools
- ✓ Praktischer Nutzen
- ✓ Gäste WLAN prüfen
- ✓ WLAN Räumliche Abdeckung
- ✓ WLAN DeAuth Angriff
- ✓ Effiziente WLAN Angriffe (begrenzt)
- ✓ Einsatzgebiete für KARMA Sploit
- ✓ Network Access Control (NAC – 802.1X)

Unterrichteinheit	UE 37	CSH

Hacking Device
- ✓ Von Zwergen und Riesen
- ✓ Aufgaben einer Hacking Device
- ✓ Aufbau einer einfachen Hacking Device
- ✓ Bestückung eines Raspberry Pi4
- ✓ Betriebssysteme für Raspberry Pi Hacking
- ✓ Special: Raspberry Pi ohne Steckdose
- ✓ KALI Linux auf Raspberry installieren
- ✓ KALI Linux vorbereiten
- ✓ RASPI-CONFIG im Überblick
- ✓ Raspberry Pi vorbereiten
- ✓ Zugriff auf das Unternehmensnetzwerk
- ✓ Für die echten Hacker
- ✓ Inspiration für Hacking Device
- ✓ Kommerzielle Hacking Devices

Unterrichteinheit	UE 38	CSH

VLAN-Hacking & Man-in-the-Middle
- ✓ VLAN-Hacking
- ✓ GNS3: Netzwerk Emulator
- ✓ GNS3 – VLAN Hopping Szenario
- ✓ Man-in-the-Middle Angriffe
- ✓ DNS Manipulation
- ✓ Kaum MitM Potential in KALI Linux

Unterrichteinheit	UE 39	CSH

Mobile Device & Cloud Security
- ✓ Mobile Device Security – Einfach hackbar
- ✓ Indirekte Angriffe
- ✓ Mobile Device Security – Approach
- ✓ Cloud Security
- ✓ Sicherheit in den Clouds
- ✓ Fragen und Antworten

Unterrichteinheit	UE 40	CSH

Q&A und Abschlussprüfung
- ✓ Informationen zur Abschlussprüfung
- ✓ Fragen und Antworten

Weitere wichtige Informationen

Ihr Trainer: Herr Thomas Wittmann

Der Trainer dieser exklusiven Online-Ausbildungsreihe ist Herr Thomas Wittmann. Er ist seit über 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.

Optimale Prüfungsvorbereitung

Nach der Ausbildung besteht die Möglichkeit eine Prüfung abzulegen.
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.

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.